Bird & Bird

Enforcement tables by country

Australia

Date	Infringing entity	Details of infringement	Sanction(s) imposed
June 2017	The Westin Sydney ("**Westin**")	Westin interfered with the complainant's privacy by recording a telephone conversation without the complainant's knowledge (in contravention of APP 3).	Westin was required to: (a) issue a written apology to the complainant; and (b) pay the complainant AUS$1,500 (non-economic loss).
March 2017	Comcare	Comcare interfered with the complainant's privacy by: (a) disclosing personal information, including sensitive health information, on a publicly available website (in contravention of IPP 11); and (b) failing to take reasonable security safeguards against loss, access, use, modification or disclosure or any other misuse (in contravention of IPP 4). Full details of case here: http://www.austlii.edu.au/au/cases/cth/AICmr/2017/28.html	Comcare was required to: (a) pay the complainant AUS$20,000 (non-economic loss); and (b) pay the complainant AUS$3,000 as reimbursement for expenses incurred with making and investigating the complaint.
March 2017	Department of Defence ("**DOD**")	DOD interfered with the complainant's privacy disclosing the complainant's personal information in breach of APP 6 (use and disclosure of personal information). Full details of case here:	DOD was required to: (a) pay the complainant AUS$12,000 (non-economic loss); and (b) pay the complainant AUS$3,420 as

		http://www.austlii.edu.au/au/cases/cth/AICmr/2017/25.html	reimbursement for expenses incurred with making and investigating the complaint.
December 2016	Veda Advantage Information Services and Solutions ("**Veda**")	Veda interfered with the privacy of a class of individuals by: (a) not stating prominently that individuals have a right to obtain their credit reporting information free of charge (in contravention of the *Privacy (Credit Reporting) Code 2014*); (b) failing to take reasonable steps to ensure free access to credit reports were available and as easy to identify as paid reports (also in contravention of the above code); (c) using and disclosing personal information it held about individuals seeking free access to credit reports for the purpose of direct marketing (in contravention of APP 7 – direct marketing); and (d) charging for 'expedited delivery' (also in contravention of the above code). Full details of case here: http://www.austlii.edu.au/au/cases/cth/AICmr/2016/88.html	Veda was required to: (a) refund everyone affected by the 'expedited delivery' charge (for those individuals that had only requested their 'one' free report that year); (b) take necessary steps to ensure free credit reports are easy to identify; and (c) confirm and advise the Privacy Commissioner of the amendments made to the application procedure for free reports.
November 2016	Veda Advantage Information Services and Solutions ("**Veda**")	Veda interfered with the complainant's privacy by: (a) not taking reasonable steps to ensure certain credit information was accurate, up-to-date and complete; (b) using false or misleading credit information; (c) failing to give each recipient of the incorrect information notice of correction. These contraventions were dealt with under the specific credit information provisions contained in section 20P of the Privacy Act. Full details of case here: http://www.austlii.edu.au/au/cases/cth/AICmr/2016/81.html	Veda was required to: (a) issue a written apology; (b) pay the complainant AUS$10,000 (non-economic loss); (c) pay the complainant AUS$5,830 to reimburse him for expenses reasonably incurred in connection with the making of the complaint and the investigation of the complaint; and (d) review its procedures and report back within 6 months.
November	Commonwealth Bank of	CBA interfered with the complainant's privacy by disclosing her	CBA was required to:

2016	Australia ("**CBA**")	personal information to the principal of a CBA mortgage agency for a purpose other than the primary purpose of the collection. This was held in breach of NPP 2 (disclosing personal information for a secondary purpose), and CBA also failed to take reasonable steps to protect her personal information under NPP 4. Full details of case here: http://www.austlii.edu.au/au/cases/cth/AICmr/2016/80.html	(a) issue an apology; (b) pay the complainant AUS$10,000; and (c) review its information handling policies, particularly with respect to access to customer information where there is an acknowledged, or potential conflict of interests.

China

Date	Infringing entity	Details of infringement	Sanction(s) imposed
April 2017	Liu zhaohuan ("**Liu**"), Hao Zhengjia ("**Hao**")	Liu bought a large amount of citizens' personal information from his internet friends (including Hao) that he made through a QQ group in order to advertise his products. Hao bought a large amount of citizens' personal information from others and then re-sold the information to his internet friends through a QQ group for profits. Yuanshi County People's Court of Hebei Province decided that Liu and Hao committed the crime of illegally obtaining personal information of citizens.	Liu was required to: (a) pay a fine of 2,000RMB; and (b) serve a prison sentence of 6 months on probation for 1 year. Hao was required to: (a) pay a fine of 2,000RMB; (b) serve a prison sentence of 10 months on probation for 1 year; and (c) return all of his illegal income, which was confiscated.
March 2017	Tan	Tan used hacking technology to illegally invade 81 websites to download personal information of citizens and sold part of it through QQ for profits. People's Court of the Liujiang District, Liuzhou City, Guangxi Zhuangzu Autonomous Region held the decision that Tan committed the crime of illegally obtaining personal information of citizens.	Tan was required to: (a) pay a fine of 10,000RMB; (b) serve a prison sentence of 1 year and 6 months; and (c) return all of his illegal income, which was

			confiscated.
March 2017	Beijing Quna Information Technology Co., Ltd. ("**Quna**") China Eastern Airlines Co., Ltd. ("**CEA**")	Pang Lipeng ("**Pang**") commissioned Lu Chaoyong to book a flight through Quna. Xinglv Company was the ticket agent. Xinglv Company booked the ticket with CEA. Throughout the process, neither Quna, Xinglv Company, nor CEA obtained Pang's phone number. However, Pang received a scam text message from an unknown number and also received a text message about the flight from CEA. Pang claimed that Quna and CEA had disclosed his personal information. Beijing First Intermediate People's Court held that it was very likely that Quna and CEA had disclosed Pang's personal information and should take the responsibility for these actions.	Quna was required to make a public apology to Pang on their website, www.qunar.com, for 3 consecutive days and bear the relevant expenses. CEA was required to make a public apology to Pang on their website, www.ceair.com, for 3 consecutive days and bear the relevant expenses.
March 2017	Agricultural Bank 0f China Chaoyang East Branch ("**ABC**")	Cai Mingyang ("**Cai**") is a debit card owner with ABC. On 29 September 2015, he suffered identity theft on his card and lost 100,000RMB. Cai sued ABC for failing to protect his confidential information relating to the debit card. Third Intermediate People's Court of Beijing upheld the decision of the first instance. It ruled that Cai's application for a debit bank account with ABC established a creditor-debtor contractual relationship between Cai and ABC, which imposes a contractual duty on ABC to protect the creditors' rights of property. ABC, as the issuer of the card, bears the responsibility of ensuring the exclusivity and irreplaceable nature of the card. The fact that ABC paid for the fraudulent card showed that ABC failed to fulfil its contractual obligations.	ABC was required to compensate Cai for RMB 100,000, in addition to paying costs and interest.
February 2017	Liu	Liu stole courier documents from YTO Express when he received and sent packages in YTO Express. He used the personal information including the phone numbers contained in the courier documents to advertise his own company project. Jinzhou People's Court of Hebei held the decision that Liu committed the crime of illegally obtaining personal information of	Liu was required to: (a) pay a fine of 5,000RMB; and (b) serve a prison sentence of 6 months on probation for 1 year.

		citizens.	
February 2017	Hangzhou Gelaimei medical beauty hospital Co., Ltd ("**Gelaimei Hospital**")	Gelaimei Hospital put Ms. Xia's photos on its several websites for advertising and promotion of its services. Ms Xia alleged that Gelaimei Hospital has infringed her right of portrait and reputation. Chaoyang District People's Court of Beijing held that Gelaimei Hospital did not infringe Ms. Xia's right of reputation but did infringe her right of portrait.	Gelaimei Hospital was required to: (a) make an apology to Ms. Xia on the front page of their website, 8-dou.com, for 10 consecutive days consecutively; and (b) to compensate Ms. Xia's loss of 5,000RMB, in addition to other expenses.
December 2016	Yin, Liu, Yan, Zhou, Cai and Shanghai Zexi culture communication Co., Ltd ("**Zexi Company**")	Since 2014, Yan, Zhou and Cai copied citizens' personal information from their former companies and exchanged with others in order to pursue new positions at a new company. Yin, who owns Zexi Company, directed employee Liu to obtain citizens' information by exchanging for the purpose of developing his business. Xuhui District People's Court of Shanghai ruled that Yan, Zhou, Cai, Yin, Liu and Zexi Company all committed the crime of illegally obtaining personal information of citizens.	Zexi Company was required to pay a fine of 5,000 RMB. Yin was required to pay a fine of 5,000RMB, imprisonment of 6 months on probation for 1 year. Liu and Yan was required to pay a fine of 4,000RMB and serve a prison sentence of 5 months on probation for 5 months. Zhou was required to pay a fine of 8,000RMB and serve a prison sentence of 10 months on probation for 1 year. Cai was required to pay a fine of 1,000RMB and serve a prison sentence of 3 months on probation for 3 months.
December 2016	China Southern Airlines Corp., Ltd. ("**Southern Airline**")	On 24 July 2016, Wan Cun ("**Wan**") helped others to book a flight on the official website of Southern Airline, and Wan received a scam message sent by an entity claiming to be "Southern Airline" on 14 August. Due to this scam message, Wan suffered a loss of 10,800RMB. Wan sued Southern Airline for disclosing his personal information. Second Court of Guangzhou Railway-Transport rejected the claim for lack of evidence.	Claim rejected.
November 2016	Agricultural Bank of China Limited Shanghai Jiangwan Branch ("**ABC Shanghai Jiangwan Branch**")	Chen Wenchun ("Chen") is a debit card owner with ABC Shanghai Jiangwan Branch. On 21 July 2016, a text message informed Chen that a sum of 50,000 RMB was transferred from his card and a sum of 20,000 RMB was withdrawn. Chen sued ABC Shanghai Jiangwan Branch for the compensation.	ABC Shanghai Jiangwan Branch was required to pay compensation to Chen of 70,000 RMB, in addition to interest and other expenses incurred from his loses.

		Hongkou District people's Court of Shanghai judged in favour of Chen's appeal. It ruled that ABC Shanghai Jiangwan Branch had a contractual obligation to protect the creditors' rights of property free from any parties' interference. ABC Shanghai Jiangwan Branch could not prove Chen's fault of leaking the card information and password.	
November 2016	Bank of Communications Co., Ltd. Beijing Dongdan North Street Branch ("**BOC Dongdan North Street Branch**")	Sheng Li ("**Sheng**") is a debit card owner with BOC Dongdan North Street Branch. On 10 July 2016, she suffered identity theft and her card was used to make 10 payments abroad. Sheng sued BOC Dongdan North Street Branch for failing to protect confidential information relating to the debit card and claimed that it should take all the responsibility. The Second Intermediate people's Court of Beijing upheld the decision of the first instance. It ruled that Sheng's application for debit bank account with BOC Dongdan North Street Branch established a creditor-debtor contractual relation between Sheng and BOC Dongdan North Street Branch, which impose BOC Dongdan North Street Branch a contractual obligation to protect the creditors' rights of property free from any parties' interference. BOC Dongdan North Street Branch as the issuer of the card, bears the responsibility of ensuring the uniqueness and irreplaceability of the card. The fact BOC Dongdan North Street Branch paid for the fraud card showed that BOC Dongdan North Street Branch failed to fulfil its contractual obligation.	BOC Dongdan North Street Branch was required to pay compensation to Sheng of77,030.29RMB, in addition to the costs and interest.
November 2016	Shanghai Meilai Medical Beauty Clinic Co., Ltd ("**Meilai**")	Meilai put Ms. Wang's photos in an article on its website to promote Meilai's plastic surgery project and Ms. Wang alleged that Meilai Hospital has infringed her right of portrait and reputation. Dongcheng district People's Court of Beijing held the decision that Meilai did not infringe Ms. Wang's right of reputation but infringed her right of portrait.	Meilai was required to: (a) make an apology on the front page of the website for 7 days; and (b) pay compensation to Ms. Wang for 6,000RMB, in addition to other expenses.
October 2016	Yang Zhaohua ("**Yang**")	Yang and his partner logged on the phishing website and stole the bank card information including customer name, ID number, bank card number, mobile phone number, and other information, for profits.	Yang was required to: (a) pay a fine of 30,000RMB; (b) serve a prison sentence of 3 years; and

		Yuzhong District People's Court of Chongqing upheld the decision that Yang committed the crime of illegally obtaining personal information of citizens	(c) pay back all of his illegal income, which was confiscated.

Czech Republic

Date	Infringing entity	Details of infringement	Sanction(s) imposed
May 2017	EURYDIKAPOL, s. r. o. ("**Eurydikapol**")	The Czech DPA imposed a record fine in the amount of CZK 4,250,000 (approx. EUR 162,337) on the Eurydikapol for the distribution of unsolicited commercial communications. The DPA imposed the fine on the basis of around 700 complaints. Eurydikapol was sending unsolicited commercial communications without consents of the addressees that were not even the company's clients. These activities of the Eurydikapol were highly problematic because commercial communications were sent in large numbers, and in one case almost 200 e-mails were delivered.	Eurydikapol were subject to a fine of CZK 4,250,000 (approx. EUR 162,337)

Denmark

Date	Infringing entity	Details of infringement	Sanction(s) imposed
April 2017	Danish Patient Safety Authority	The DPA found that the Danish Patient Safety Authority had failed to comply with § 41 of the Danish Data Protection Act, by posting 900 pages of health data online.	No sanction was imposed.
April 2017	The Board for IT and	The Board has failed to comply with § 41 of the Danish Data Protection Act, as their EASY-P (administration system for technical	The DPA is awaiting a response from STIL as to whether the security breach has been used for unauthorized access

	Learning	schools) insufficiently provided protection for personal identification numbers and the names attached thereto. They were available to anyone having access to the system. The system therefore did not provide for appropriate security measures.	to the personal identification numbers or other personal data. No sanction has yet to be imposed.
April 2017	The Social Appeals Board	The Social Appeals Board has failed to comply with § 19 of the Danish Security Executive Order regarding logging of data in connection with the production of statistics.	No sanction was imposed as the Board expects to be compliant with requirements in § 19 as of 1 July 2017.
April 2017	The Danish Institute for Local and Government Research	The institute failed to live up to the requirement in § 19 of the Danish Security Executive Order, as they carried out mechanical logging of users without scrambling the personal data included in i.e. observation and interview data.	No sanction was imposed as the institutes' data processing now is compliant with the Danish Security Executive Order.
March 17	Danish Supermarket	Danish Supermarket has failed to comply with the Danish Act on the Processing of Personal Data as it has not given a complainant and her son access to video material, which contains footage of the complainant's son.	The supermarket was required to give the complainant and her son access to the video footage.
March 17	The Region of Central Jutland	As a result of an inspection, the DPA has criticized the region for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •non-compliance with the requirement of annual reviews and updates on security rules •lack of guidelines regarding supervision •lack of written data processing agreements •lack of control with the data processor	The DPA has requested a report on how the region intends to comply with Danish data protection regulations in the future.
March 17	The Region of Zealand	As a result of an inspection, the DPA has criticized the region for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •lack of guidelines regarding supervision •lack of written data processing agreements •lack of control with the data processor	The DPA has requested a report on how the region intends to comply with Danish data protection regulations in the future.

March 17	The Region of Northern Jutland	As a result of an inspection, the DPA has criticized the region for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •non-compliance with the requirement of annual reviews and updates on security rules •lack of guidelines regarding supervision •lack of control with the data processor	The DPA has requested a report on how the region intends to comply with Danish data protection regulations in the future.
March 17	The Region of Southern Denmark	As a result of an inspection, the DPA has criticized the region for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •non-compliance with the requirement of annual reviews and updates on security rules •lack of guidelines regarding their own supervision •lack of written data processing agreements •lack of control with the data processor	The DPA has requested a report on how the region intends to comply with Danish data protection regulations in the future.
March 17	The Capital Region of Denmark	As a result of inspection, the DPA has criticized the region for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •non-compliance with the requirement of annual reviews and updates on security rules •lack of guidelines regarding supervision •lack of control with the data processor	The DPA has requested a report on how the region intends to comply with Danish data protection regulations in the future.
January 17	Strandmølleskolen	The DPA found that a school's review of a number of students search history on their private computers was in violation of § 5 and § 6 of the Danish Data Protection Act.	No sanction was imposed.
November 16	Læsø Municipality	As a result of an inspection, the DPA has criticized the municipality for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •lack of guidelines regarding supervision •insufficient authorization •lack of written data processing agreements •lack of control with the data processor	The DPA has requested a report on how the municipality intends to comply with Danish data protection regulations in the future.

November 16	Odense Municipality	As a result of an inspection, the DPA has criticized the municipality for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •lack of guidelines regarding supervision •non- compliance with § 19 of the Danish Security Executive Order •insufficient authorization •lack of written data processing agreements •lack of control with the data processor	The DPA has requested a report on how the municipality intends to comply with Danish data protection regulations in the future.
November 16	Rudersdal Municipality	As a result of an inspection, the DPA has criticized the municipality for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •non-compliance with § 19 of the Danish Security Executive Order •lack of written data processing agreements •lack of control with the data processor	The DPA has requested a report on how the municipality intends to comply with Danish data protection regulations in the future.
November 16	Vejle Municipality	As a result of an inspection, the DPA has criticized the municipality for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •non-compliance with the requirement of annual reviews and updates on security rules •insufficient authorization •lack of control with the data processor •lack of satisfactory cooperation with the inspection	The DPA has requested a report on how the municipality intends to comply with Danish data protection regulations in the future.
November 16	Kerteminde Municipality	As a result of an inspection, the DPA has criticized the municipality for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: •non-compliance with § 19 of the Danish Security Executive Order •insufficient authorization •lack of control with the data processor	The DPA has requested a report on how the municipality intends to comply with Danish data protection regulations in the future.
November 16	Odder Municipality	As a result of an inspection, the DPA has criticized the municipality for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the:	The DPA has requested a report on how the municipality intends to comply with Danish data protection regulations

		• non-compliance with the requirement of annual reviews and updates on security rules • non-compliance with § 19 of the Danish Security Executive Order • insufficient authorization • lack of control with the data processor	in the future.
November 16	Langeland Municipality	As a result of an inspection, the DPA has criticized the municipality for its failure to comply with the Danish Data Protection Act and Danish Security Executive Order. The DPA was critical of the: • non-compliance with the requirement of elaborating and updating security rules annually • lack of guidelines regarding supervision • non-compliance with § 19 of the Danish Security Executive Order • lack of control with the data processor • lack of satisfactory cooperation with the inspection	The DPA has requested a report on how the municipality intends to comply with Danish data protection regulations in the future.

France

Date	Infringing entity	Details of infringement	Sanction(s) imposed
June 2017	Ruling of the social chamber of the French *Cour de cassation* (French Court of cassation) **Mr X / Pergam**	In 2008, Mr X was hired as a Finance and Administrative manager at Pergam. In May 2010, he was laid-off for professional incompetence and brought the case to the Court to contest his termination. The former employer provided emails exchanged between Mr X and the Management. Mr X claimed that the emails provided to the proceedings by his former employer, could not be considered as legal evidence. Mr X argued that the contentious emails came from the company's professional messaging system, which constitutes a data processing and should have therefore been notified to the CNIL. As his former employer did not notify the processing to the	The Court overruled the decision of the Court of appeal and refer the case back to a new Court of appeal for judgment.

		CNIL, the emails could not be considered as legal and should be removed from the proceedings. The Court of Appeal of Paris followed Mr X's argument, in accordance with current French case-law, ruled that the emails should be removed as the messaging system of the company had not been notified to the CNIL. The evidence was deemed to be illegal. The company brought the case to the Court of cassation which overruled the decision of the Court of appeal. The Court set aside the decision as the professional messaging system was not provided with an individual control system of employee' activities. In this regard, the Court of cassation considered that the messaging system should have been notified to the CNIL but only through a simplified notification. For this reason, the Court deduced that the professional messaging system did not prejudice the employees' privacy and the emails could be provided to the proceedings as a legal means of evidence.	
May 2017 (n° SAN-2017-008)	Decision of the CNIL (French Data Protection Authority) **CABINET DENTAIRE X**	Mr X is a dentist and runs his dental office with two employees. In November 2015, the CNIL received a complaint from a former patient of Mr X who did not receive an answer following his request to access to his medical record. In January 2016, the CNIL sent a letter to Mr X to be provided with more information about the patient's access request. As Mr X did not answer, the CNIL sent two additional letters by registered post with acknowledgement of receipt, in March and April 2016. In October 2016, the CNIL issued a formal notice against Mr X requesting to comply with his obligations within a 1 month period. Namely, Mr X was required to set up an effective procedure of access request when patients wish to get access to their medical record. Mr X was also required to provide the plaintiff with a copy of his	The CNIL imposed a €10 000 fine against Mr X due his failure to respect the right of access of his former patient. This sanction was also made public in order to raise awareness of data subjects about their rights and bring the data controllers' attention to take seriously the CNIL's requests.

		medical record. As the CNIL did not receive any answer from Mr X, the disciplinary proceedings undertaken against Mr X led the CNIL to highlight the breaches including, on the obligation for right of access, that although the dentist provided his former patient with his medical record after the notification of the disciplinary proceedings, the CNIL observed that the dentist did not grant the patient's access request within the allocated time limit. The CNIL also considered that the ethical duty related to medical confidentiality cannot be opposed to the patient's right of access. This situation led to deprive the patient with the opportunity to transmit information about his medical condition to his new practitioner. In relation to the breach to the obligation to respond to the CNIL's requests, the CNIL noted that Mr X did not provide any answer to the CNIL. For this reason, the CNIL considered that Mr X's behaviour demonstrates an absence of interest regarding the issues related to data protection and the respect of the French DP Act.	
April 2017 (n° SAN-2017-002)	Decision of the CNIL (French Data Protection Authority) **ALLOCAB**	Allocab provides car-hire/ motorcycle taxi services with drivers. Under the same name, the company operates the www.allocab.com website along with a mobile app. In January 2015, the CNIL received a complaint against Allocab from a client who denounced the retention of his/her credit card data at the time of final payment. In March 2015, the CNIL performed an onsite inspection in the premises of the company and observed several breaches of the French DP Act. In November 2015, the CNIL issued a formal notice against the company requesting to comply with its obligations within a period of 3 months. Namely, Allocab was required to set up a data retention policy in particular to ensure that data related to the security codes	The CNIL imposed a € 15 000 fine on Allocab due to its several breaches of the French DP Act. The sanction was also made public due to the persistence of the breaches. The CNIL also considered relevant to raise awareness of data controller to take seriously the CNIL's requests and adopt effective measures.

		will not be retained after the final transaction and to make sure to supress data related to clients' accounts upon their requests. The CNIL also required the company to take necessary measures to guarantee security and confidentiality of users' personal data, in particular by strengthening clients' passwords. By letter dated April 2016, the company indicated that it had complied with the requests of the CNIL. In July 2016, the CNIL requested further information from the company as the CNIL considered that the company did not comply with all the requests. In September 2016, the CNIL sent a reminder as the company failed to answer to the CNIL. By letter dated September 2016, the company indicated that had taken further steps to be in compliance with the CNIL's requests. In December 2016, the CNIL performed a second onsite inspection in the premises of the company and observed that several issues were still not remedied. The disciplinary proceedings undertaken against the company led the CNIL to highlight the following breaches : (a) the failure to set up a data retention policy: The CNIL noted that even though the company purged some client accounts, a certain numbers remain active and some security codes were still retained after the deadline set up in the formal notice. (b) the breach of the data security obligation: The CNIL noted that Allocab did not ensure the security and confidentiality of data because of certain weakness in passwords' management such as password in plain text in the confirmation email of the account creation.	
March 2017	Ruling of the French *Cour d'appel* of Paris	Free is a French Internet Service Provider. Buzzee edits software and provides companies with unified messaging, telephony, fax,	The Paris Court of Appeal upheld the lower court's decision in that it ordered Free to unblock IP address

(n°16/03440)	(Court of Appeal of Paris) **Free / Buzzee**	conference call and postal mail solutions. Free had blocked mail servers of Buzzee considering that Buzzee had been sending spam messages to non-professional e-mail addresses such as 'name.surname@free.fr'. Buzzee was in the position of being unable to send messages to recipients with a Free email address. On the basis of article L. 34-5 of the French Post and Electronic Communications Code (PECC), Free argued that it is its responsibility to protect users against the unfair and unlawful collection of personal data by Buzzee and against the sending of large numbers of e-mails without the user's prior consent, and without possibility to oppose.	servers of the company Buzzee. The Court considered that Free is not responsible for ensuring that article L. 34-5 of the PECC is complied with as this responsibility falls within the scope of the CNIL. Pursuant to article L. 34-5 of the French PECC, the individual's contact details cannot be used for direct email marketing purposes without having obtained its prior specific consent (the opt-in principle). Free interpreted this provision as authorising it to block the sending of massive amount of e-mails from Buzzee. However this interpretation is inconsistent with the spirit of article L. 34-5 of the French PECC.
February 2017 (n°393714)	Ruling of the French *Conseil d'Etat* (Administrative Supreme Court) **JC Decaux**	JC Decaux is a company specialized in urban advertising through street furniture. The company submitted a request for authorization to the CNIL in relation to a data processing aimed at testing a quantitive evolution methodology of pedestrian flows for 4 weeks on the Esplanade at La Défense. The project consisted in exploiting wi-fi counting boxes placed on the company's advertising hoardings, in order to capture MAC addresses of mobile devices within a radius of 25 meters, and then to calculate geographic positioning. The CNIL refused to grant the authorization. Indeed, the CNIL pointed out that the company built all its project from the premise	The French Administrative Supreme Court rejected the JC Decaux's request and confirmed the CNIL's decision. It held that: (a) The personal data were collected directly even though the collection did not necessitate the data subjects' intervention. Therefore, the CNIL applied the provision of the article 32 of the French DP Act related to the direct data collection. (b) The Court approved the CNIL's interpretation considering that the anonymisation techniques were not sufficient to prevent the identification of data subjects. The Court also considered that the data processing purpose was to identify the movement of

		that the technique used enabled to anonymise the data collected. However, the CNIL considered that the purposes of the project aimed not only to evaluate the number of individuals crossing the Esplanade at La Défense but also to estimate the number of passers-by, their itinerary, and the number of times a passer-by cross the Esplanade over a period of time. According to the CNIL, the purposes of the project were incompatible with an anonymisation of data collected. Since the data were not anonymised, the CNIL highlighted that the data processing should respect the rights of individuals and that individuals should be provided with an information notice in accordance with article 32-I of the French DP Act (case in which data are collected directly from the data subject). The CNIL considered that these conditions were not met. The company challenged the CNIL's decision before the French Administrative Supreme Court.	people and their frequency on the esplanade of La Défense. The Court concluded that the purposes of the data collection were incompatible with the anonymisation of the collected data. (c) The CNIL noted that the data processing was subject to the provisions of the French DP Act regarding the information since the techniques proposed by the company would not render the data anonymous.
January 2017 (n°SAN-2017-001)	Decision of the CNIL (French Data Protection Authority) **Carrefour Banque**	Carrefour Banque is the European subsidiary bank of Carrefour SA, and is specialized in offering credit solutions. In October 2015, the CNIL received a complaint against the company from a person who signed up to a loan with Carrefour Bank. She denounced her inscription in the national registry of credit reimbursement default concerning individuals (*Fichier national des Incidents de Remboursement des Crédits aux Particuliers* – FICP) operated by *the Banque de France* (bank of the French State). The non-payments related to the overdrafts and loans are compiled in that registry. It is consulted by the banks before granting loans to individuals. The CNIL obtained a copy of the plaintiff's inscription which stated the subscription of the plaintiff for revolving credit with a reference date on 3 October 2012. In December 2015, the CNIL requested the company to provide explanations regarding the contentious situation. By letter dated February 2016, the company indicated that the plaintiff's inscription in May 2012 was related to the non-payment of two credit due dates. Due to another non-payment in July 2012, the plaintiff was registered again. Another inscription was made due to a default of	The CNIL issued a public warning against Carrefour Banque based on the number of data's subjects affected, the persistence of the breach and the national role of the FICP in the over-indebtedness avoidance.

		payment in October 2015. Further to another request made by the CNIL to the Banque de France, the CNIL was informed that the plaintiff was registered for a revolving credit with a reference date of 13 May 2012. The proceedings conducted by the CNIL revealed that the plaintiff's name appeared three times in the registry. In August 2016, the CNIL conducted an onsite inspection in the premises of the company in order to proceed with the complaint. By letters dated October 2016, the company provided explanations on its process regarding direct debit of regularization. This correspondence confirmed the existence of a dysfunction regarding the inscription to the FICP since May 2010. The dysfunction leaded to the suppression of registration and reregistration of 38 329 individuals. The company revealed that correctives steps had been taken and 5 644 individuals remained affected. Despite the counter arguments raised by the company, the CNIL highlighted the following breach: - Breach of the obligation to process accurate and up-to-date data: the CNIL noted that the company failed to implement corrective actions as the dysfunction was fixed one year after it was detected by the company. The CNIL also considered that the company did not comply with its obligations as it processed inaccurate data for a long period of time.	
December 2016 (n°2016-406)	Decision of the CNIL (French Data Protection Authority) **Meetic SAS**	Meetic SAS operates the dating website www.meetic.fr, available in almost all European countries. In November 2014, the CNIL performed two onsite inspections on the company's premises, and observed several breaches of the French DP Act. In May 2015, the CNIL also conducted an online inspection of the company's website.	The CNIL imposed a €20 000 administrative fine on Meetic based on the nature and volume of data processed. The sanction was also made public due to the seriousness of the breach of law and the need to inform internet users and data controller of their rights and obligations under the French DP Act.

		In June 2015, the CNIL issued a formal notice, summoning the company to take necessary steps to remedy the situation: in particular, the company was required to attain the prior and informed consent of its users in order to collect and process sensitive data related to racial or ethnic origins, religious beliefs or sex life. Regarding sensitive data, the CNIL noted that such consent could be obtained by a tick-box. The CNIL found that the users' consent for the processing of their sensitive data was collected at the moment of their registration on the website by ticking one single box for three distinct items of information: 1) the age of majority requirement, 2) agreement to the terms of use, and 3) the processing of data related to sexual orientation. As such, the CNIL considered that this could not be regarded as the expression of explicit consent by the data subjects. With two letters, both dated October 2015, the company presented steps taken to comply with the formal notice. A meeting was also organised with the CNIL at the company's request, and additional time was granted until January 2016. Despite these steps, the CNIL observed that several issues were still not remedied : As for the breach of the obligation to collect data subjects' consent to process sensitive data, the CNIL recalled that the processing of sensitive data is prohibited unless the data subject has given his/her express consent, rejecting the counter-arguments raised by Meetic SAS regarding the interpretation of this consent. The CNIL argued that obtaining consent and the express nature of this consent must be strictly interpreted; that is, consent is expressed when the data subject indicates his/her consent to the processing of his/her sensitive data by a positive action. The CNIL also pointed out that the tick box provided on the company's website only referred to sexual orientation: in this regard, the tick box could not enable data subjects to give their express consent to the processing of data related to either racial or ethnic origins, or their religious beliefs. The CNIL also noted that the company failed to comply with its obligations within the time allocated, despite the personalized support it received.	

December 2016 (n°2016-405)	Decision of the CNIL (French Data Protection Authority) **Samadhi SAS**	Samadhi is the company which operates www.attractiveworld.net dating website. In July and October 2014, the CNIL conducted two onsite inspections on the premises of the company, observing several breaches of the French DP Act. In June 2015, the CNIL issued a formal notice against the company requesting it to comply with its obligations within a period of 3 months. Namely, the company was required to inform data subjects about the processing of sensitive data related to their sexual orientation. The CNIL considered that explicit consent can only be obtained by using a tick-box, and voluntary provision of sensitive data by users is not sufficient to be considered as valid consent in accordance with the French DP Act. By three letters dated August, September and October 2015, the company communicated the steps it has taken to comply with the requirements of the formal notice, and asked for an extension. Considering that the company partially remedied the situation, the CNIL granted this extension until January 2016. Even though the company took some steps to remedy to the situation, the adopted measures were not deemed sufficient by the CNIL. In a reminder sent on April 2016, the CNIL pointed out that the company did not answer to the consent issue, and noted that the level of compliance was still insufficient. Considering that the measures were not consistent, the CNIL to highlight a failure to fulfil the obligation to collect data subjects' prior consent for the processing of sensitive data in the subsequent disciplinary proceedings; rejecting the counter-arguments raised by the company, the CNIL recalled that express consent must be collected to process sensitive data. In its view, inserting a specified tick-box related to sensitive data is deemed to comply with the	The CNIL imposed a €10 000 administrative fine on Samadhi based on the nature and the volume of data processed. The sanction was also made public due to the seriousness of the breach of law and the need to inform internet users and data controller of their rights and obligations under the French DP Act.

		French DP Act provisions. The CNIL emphasized that this requirement was brought to the attention of the company in its reminder, and that the steps taken by the company during the disciplinary proceedings cannot retroactively undo the established breach of law. The CNIL also noted that spontaneously providing data related to sexual orientation cannot be considered as the expression of an affirmative consent.	
November 2016 (n°15-22.595)	Ruling of the civil chamber of the French *Cour de cassation* (French Court of cassation) **Cabinet Peterson / Groupe Logisneuf et autres**	Logisneuf is a real estate business group that specializes in selling new-build housing through its website www.logisneuf.com . Peterson, a competitor of Logisneuf, offers real estate expertise. Three companies of Logisneuf noticed connections from external computers using company administrator codes on their internal computer network. As a result, the three companies filed a complaint before the judge to obtain, from several Internet service providers, the identities of the contentious IP address owners. The measure of inquiry revealed that the computers were owned by its competitor, the Peterson company. Challenging the legality of the measure of inquiry, Peterson filed a complaint before the same judge requesting to retract his judicial decision. Dismissed in his claim, Peterson appealed the case: Peterson argued that the retention of IP addresses should have been notified to the CNIL. In the absence of such notification, Peterson argued that the measure of inquiry should be considered as illegal. The appeal court did not side with this interpretation, stating that the IP address was not personal data since such data relates to a computer rather than its user; therefore, the court judged that the French DP Act provisions were not applicable. However, when the case reached the French Supreme Court, the judges overruled the decision and stated that the IP addresses which allow the indirect identification of an individual are in fact personal data. In this regard, collecting an IP address is considered data	The Supreme Court overruled the appeal decision and stated that IP addresses constitute personal data and must be subjected to the French DP Act.

		processing, and the CNIL must be notified as such.	
October 2016 (n°2016-315)	Decision of the CNIL (French Data Protection Authority) **Parti Socialiste**	The Socialist Party (hereinafter "PS") is one of the main political parties in France, with approximately 111 450 members. In May 2016, the CNIL was informed of the existence of a security breach that lead to a data leak on the PS's website. The CNIL conducted an online inspection and observed that new members' data, registered into the payment tracking platform, could be freely accessed by entering a specific URL. The same day, the CNIL alerted the PS about this data security breach. In June 2016, the CNIL performed an onsite inspection on the premises of the PS and observed that a JavaScript infection in a registration form was the source of the data security breach. In addition, the CNIL pointed out that no data retention policy was set up. The PS indicated that it had taken corrective measures as soon as it has been alerted by the CNIL about the breach. The disciplinary proceedings undertaken against the PS led the CNIL to highlight the following breaches : - As to the breach of the data security obligation: The CNIL reiterated the large scope of the security breach, which affected around 70,000 new members. The CNIL noted that the seriousness of the breach was also characterized by the nature of data concerned; namely, the political opinions of affected users. The CNIL noted that the PS did not take even elementary security measures, and employed an authentication system that was both unreliable and obsolete. Recently, the CNIL deemed that the PS did not implement a connection tracking system within the members' payment platform.	The CNIL issued a public warning against the Socialist Party based on the volume and nature of the data security breach.

		- As to the breach of the obligation to determine a data retention policy: During the onsite inspection, the CNIL observed that no data retention policy was set up which was confirmed by the PS. The CNIL recalled that an indefinite retention period of data is prohibited, but that does not necessitate the destruction of said data: archiving data with limited access could be deemed acceptable. The CNIL also noted that compliance with the obligation to determine and set up a data retention period would have limited the scope of the security breach.	

Germany

Date	Infringing entity	Details of infringement	Sanction(s) imposed
March 2017	Credit rating agency Bürgel Wirtschaftsinformationen GmbH & Co.KG ("**Bürgel**")	The Hamburg Data Protection Commissioner, Johannes Caspar, issued a fine of EUR 15,000 against a credit rating agency, Bürgel, based in Hamburg. Bürgel provided a credit score to its customer based only on the home address of the concerned individual. The Data Protection Commissioner holds such transmission of personal data to be unlawful. This is due to the fact that, for the purpose of deciding on the creation, execution or termination of a contractual relationship with the data subject, a probability value for certain future action by the data subject may be calculated or used only if further data (in addition to address data) are integrated to calculate the probability value. The DPA criticized such practices, stating that the poor payment practices of others in the neighbourhood may have impacted the credit-worthiness of the data subject, even if that subject was personally solvent. In its judgment, dated 16 March 2017, the District Court of	The Hamburg Data Protection Commissioner imposed a fine of EUR 15,000 against Bürgel.

		Hamburg confirmed the decision of the Hamburg Data Protection Commissioner, including the amount of the fine to be paid (NB: the proceeding is pending because Bürgel has filed an appeal).	

Hong Kong

Date	Infringing entity	Details of infringement	Sanction(s) imposed
June 2017	Registration and Election Office ("**REO**")	Two computers holding the personal data of 3.7 million voters have been reported stolen by the city's Registration and Electoral Office. The first notebook computer contained the names of Election Committee members ("EC members") only. Given that the names of EC members are public data, and a name alone is not considered as sensitive personal data, the Privacy Commissioner took the view that harm would not be done to the EC members even when their names were leaked as a result of the loss of the first notebook computer. Therefore, the Privacy Commissioner concluded that the REO did not contravene Data Protection Principle ("DPP") 4(1) of the Ordinance for the loss of the first notebook computer The second notebook computer contained, in addition to the names and addresses available to the public in the Registers of Electors, the Hong Kong Identity Card number of all Electors; this information is considered sensitive personal data, and would not have been accessible by members of the public. The result of this investigation shows that the REO lacked the requisite awareness and vigilance expected of it in protecting personal data, rules of application and implementation of various guidelines were not clearly set out or followed, internal communication was less than effective; thus REO failed to take all reasonably practicable steps in consideration of the actual circumstances and needs to ensure that the Electors' personal data was protected from accidental loss, thereby contravening DPP 4(1) of the Ordinance.	The Privacy Commissioner served an enforcement notice on the REO pursuant to section 50(1) of the Ordinance to remedy and prevent any recurrence of the contravention. The REO is directed to: • prohibit the download or use of Geographical Constituencies electors' personal data (except their names and addresses) for the purpose of handling enquiries in Chief Executive Elections; and issue notice on this to the relevant staffs on a regular basis; • set internal guidelines in respect of the processing of personal data in all election-related activities, including: o technical security measures (information system encryption and password management); o physical security measures; o administrative measures on the use of notebook computers and other portable storage devices; and o implement effective measures to ensure staffs' compliance with the above policies and guidelines.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
December 2016	Ball Watch (Asia) Company Limited	A watch company (**Ball Watch (Asia) Company Limited**) faced two charges under the Personal Data (Privacy) Ordinance (the "Ordinance"). The first charge related to the offence of using the personal data of a data subject in direct marketing without taking specified actions and obtaining his consent, contrary to section 35C of the Ordinance. The other charge related to the offence of failing to inform the data subject when using his personal data in direct marketing for the first time of his right to request not to use his personal data in direct marketing without charge, contrary to section 35F of the Ordinance.	Fined HK$8,000 respectively for each charge; HK$16,000 in total

Hungary

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
March 2017	**EOS KSI Magyarország Inkasszó Kft** ("**EOS Kft**")	EOS Kft was established in 1997 under the name of Kasolvenzia Kft. EOS Kft has been a member of the international EOS Group since 1999. EOS Kft's main scope of business is debt recovery. The NAIH received many complaints, whereby EOS Kft had called third parties (who have not been in any contractual relationship with EOS Kft), and even sent threatening messages to them. The NAIH established that EOS Kft's data processing practice was unlawful, and ordered EOS Kft to both pay a fine and amend its data processing practice in accordance with the Privacy Act. EOS Kft initiated a judicial review against the NAIH decision. <u>Judicial review against the NAIH decision</u> The court established that the NAIH failed to establish the factual background of the case (e.g. the NAIH did not take into account that EOS Kft is different from EOS Zrt, which had a separate call centre and kept reports separately from EOS Kft); the NAIH failed to examine EOS Kft's privacy policy and did not take into account the number of data subjects). The court repealed the NAIH's first decision and ordered the NAIH to conduct new proceedings. Based on the court decision, the NAIH conducted new proceedings, where it also heard expert evidence. Under the new proceedings, the NAIH established the following: <u>Processing personal data of data subjects who are not in a contractual relationship with EOS Kft</u> The NAIH established that EOS Kft did not provide information to data subjects in connection with relevant data processing. Based on this, the NAIH established that EOS Kft infringed the right of data subjects in relation to providing information on data processing in advance.	The NAIH imposed a fine of HUF 800,000 (approx. EUR 2,666) on EOS Kft. Further, the NAIH ordered EOS Kft to fulfil the following obligations: – cease all "neighbouring" and/or "neighbour calling" practices; – cease processing those data subject's personal data who are not in a contractual relationship with EOS Zrt. (third person or non-debtor); – pay HUF 145,018 (approx. EUR 483) as an expert fee. The NAIH decided to publish its decision on the NAIH website. The reason for the amount of fine imposed was that the infringements affected thousands of data subjects, and EOS Kft continuously committed the infringing activities. With this decision the NAIH intended to ensure general prevention while deterring EOS Kft from committing similar infringements again. The NAIH also intended to force EOS Kft to create a lawful data protection practice.

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
		Legal basis of data processing The NAIH established that EOS Kft did not obtain the data subjects' consent; therefore, it did not have an adequate legal basis for processing personal data. Purpose of data processing The NAIH established that the legal interest of EOS Kft does not provide a reason for EOS Kft to process personal data of data subjects who are not in a contractual relationship with EOS Kft. There is no legal purpose which would require processing personal data (name, phone number, address) of data subjects who are not in a contractual relationship with EOS Kft. This also constitutes unnecessary intervention into privacy. Based on the above, the NAIH established that EOS Kft infringed the principle of data minimisation, and the principle of processing personal data for specified purpose.	

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
March 2017	**EOS Faktor Magyarország Zrt.** ("**EOS Zrt**")	EOS Zrt was established in 2007 in Hungary. The main scope of business EOS Zrt is debt purchase. EOS Zrt's main target groups are: the bank sector, utilities, the telecommunications sector, and trading companies. EOS Zrt is a member of the international EOS Group. The NAIH received many complaints, according to which EOS Zrt called third persons (who have not been in any contractual relationship with EOS Zrt), and even sent threatening messages to them. The complainants asked EOS Zrt to delete their personal data (name and phone number), but EOS Zrt rejected doing so. The NAIH also received a complaint from a debtor, according to which he/she received threatening calls from EOS Zrt late at night, and EOS Zrt even called the complainant's neighbour in order to forward EOS Zrt messages to the complainant. The NAIH examined not only the received complaints, but also EOS Zrt's general data processing practice with respect to third persons (non-debtors). The NAIH established that EOS Zrt's data processing practice is unlawful, and ordered EOS Zrt to pay a fine, and amend its data processing practice according to the Privacy Act. EOS Zrt initiated a judicial review against the NAIH's decision. <u>Judicial review against the NAIH's decision</u> The court established that the NAIH failed to establish the factual background of the case (e.g. the NAIH did not take into account that EOS Zrt had a separate call centre and kept its reports separately from EOS KSI Magyarország Inkasszó Kft (EOS Kft); the NAIH also failed to examine EOS Zrt's privacy policy, and it did not take into account the number of data subjects). The court repealed the NAIH's first decision and ordered the NAIH to conduct new proceedings. Based on the court decision, the NAIH conducted new proceedings, where it also heard expert evidence. Under the new proceedings, the	The NAIH imposed a fine of HUF 600,000 (approx. EUR 2,000) on EOS Zrt. Further, the NAIH ordered EOS Zrt to fulfil the following obligations: – cease all "neighbouring" and/or "neighbour calling" practices; – cease processing those data subject's personal data who are not in a contractual relationship with EOS Zrt. (third person or non-debtor); – pay HUF 151,876 (approx. EUR 506) as an expert fee. The NAIH decided to publish its decision on the NAIH website. The reason for the amount of fine imposed was that the infringements affected many data subjects, and EOS Zrt committed the infringing activities on an on-going basis. The NAIH also took into account the size and market position of the infringing entity. With this decision the NAIH intended to ensure general prevention and deter EOS Zrt from committing similar infractions again. The NAIH also intended to force EOS Zrt to create a lawful data protection practice.

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
		NAIH established the following: Processing personal data of data subjects who are not in a contractual relationship with EOS Zrt. The NAIH established that EOS Zrt did not provide information to data subjects regarding the purpose of data processing, who would process their personal data, and the fact that phone conversations will be recorded. On this basis, the NAIH established that EOS Zrt infringed the rights of data subjects in relation to providing information on data processing in advance. Legal basis of data processing The NAIH established that EOS Zrt did not obtain the data subjects' consent; therefore, it did not have an adequate legal basis for processing personal data. Purpose of data processing The NAIH established that the legal interest of EOS Zrt (namely to collect debt from debtors) does not provide a legal basis for EOS Zrt to process personal data of these persons. There is no legal basis which would require processing personal data of data subjects who are not in a contractual relationship with EOS Zrt. Objecting against the data processing The NAIH established that EOS Zrt's practice- according to which EOS Zrt rejected deleting personal data of third persons or requested to be provided more personal data in order to do so - was totally unacceptable. Examining EOS Zrt's privacy policy The NAIH established that EOS Zrt's privacy policy only included wording of the Privacy Act, and did not include any specific provisions regarding the relevant data processing. It did not include any provision according to which EOS Zrt could have requested further personal data in order to delete third persons' personal data. Based on the above, the NAIH established that EOS Zrt infringed the	

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
		principle of data minimisation, and the principle of processing personal data for specified purpose.	
March 2017	**REAL-GOLF Kereskedelmi, Szolgáltató és Ingatlantanácsadó Kft "forced cancellation"** ("**REAL-GOLF**")	The NAIH received a complaint, according to which the complainant' employment relationship with REAL GOLF ceased on 30 November 2014. Despite the fact that the complainant did not work at REAL-GOLF, REAL-GOLF reported the complainant's data to the tax authority as he/she was employed by REAL-GOLF. Processed personal data The NAIH established that the tax authority keeps public records containing employment data. Data included in the public records should be considered valid. (The contrary thereof can also be proved.) The NAIH established that REAL-GOLF reported the complainant's personal data to the tax authority despite the fact that REAL-GOLF had not been employing the data subject. This should be considered as an infringement. Legal basis of data processing The NAIH established that REAL-GOLF did not have any legal basis to transfer the data subject's personal data to the tax authority. This means that REAL-GOLF unlawfully processed the complainant's personal data.	The NAIH ordered the REAL-GOLF to fulfil the following obligation: – delete all personal data processed without any legal basis within 30 days and to provide evidence of deletion to the NAIH. The reason for no fine being imposed was that the NAIH established that REAL-GOLF is classified as an SME. As the NAIH did not establish any infringement committed by REAL-GOLF before, NAIH only warned REAL-GOLF.
December 2016	**OTP Bank Nyrt.** ("**OTP Bank**")	The OTP Group is one of the leading financial service providers in Hungary. OTP Bank is a member of the OTP Group. OTP Bank is one of the market leading credit institutions in Hungary and provides a wide range of financial services. To obtain any financial service, a contract should be concluded with OTP Bank, where personal data should also be provided. The NAIH received a complaint, according to which OTP Bank failed to provide information to the complainant in relation to data processing. The complainant further requested information related to data processing (purpose of data processing and the personal data processed), but OTP Bank failed to provide the full requested	The NAIH imposed a fine of HUF 1,000,000 (approx. EUR 3,333) on OTP Bank. Further, the NAIH ordered OTP Bank to fulfil the following obligations: – refrain from processing any personal data without legal basis; – delete all personal data processed without legal basis,

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
		information to the complainant. The complainant requested information from OTB Bank concerning the data processing, and also asked why OTP Bank handled his/her request as a complaint and not as an information request. Legal basis and duration of data processing The NAIH established that OTP Bank did process the complainant's personal data after the retention period had expired. Due to this fact, OTP Bank processed the personal data without any legal basis. Right to request information in relation to data processing In the NAIH's opinion, if the data controller processes personal data for purposes other than those specified, the data controller shall provide information separately in case of each data processing purpose. The NAIH established that OTP Bank failed to provide clear rationale for the purpose and duration of such data processing, and also failed to provide information concerning the activity carried out by the individual data processor in each case. Processed personal data The NAIH established that the OTP Bank violated the necessity-proportionality principle and the requirement of processing full, accurate and up-to-date data when processing gender data, and data on the previous address of the complainant (gender data and previous address are not required to process personal data in this case). OTP Bank's liability as data controller The NAIH established that OTP Bank as the data controller is liable for any act carried out by the employees of OTP Bank. Therefore, OTP Bank is liable for the inadequate information provided to the data subject as a result of any administrative failure.	along with personal data which is not required to achieve the purpose of data processing; – amend its data processing practice in accordance with the Privacy Act; – publish this decision on its website. The reason for the amount of fine imposed was that OTP Bank failed to provide information on data processing upon explicit request of the person whose personal data was the subject of such processing, despite the fact that the data subject submitted his/her request for information least three times; OTP Bank committed the infringement continuously over a long period of time. Further, the NAIH intended to ensure special prevention and prevent OTP Bank from committing similar infringements again. The NAIH also intended to force OTP Bank to create lawful practices with respect to providing information on data processing.

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
December 2016	**MKB Bank Zrt.** ("**MKB Bank**")	The MKB Group is one of the leading financial service providers in Hungary. MKB Bank is a member of the MKB Group. MKB Bank is one of the market leading credit institutions in Hungary, which provides a wide range of financial services. To obtain any financial services, a contract should be concluded with MKB Bank, where personal data would also be provided. The NAIH received a complaint from the complainant's legal representative, according to whom MKB Bank failed to provide information to the complainant in relation to data processing. The complainant's legal representative twice requested information related to data processing, but MKB Bank failed to provide adequate information; namely, it did not include personal data processed, and also failed to provide detailed information in relation to the circumstances under which the personal data were processed. <u>Right to request information in relation to data processing</u> The NAIH established that when first requesting information MKB Bank failed to provide any information in relation to the data processed and also included in the credit contract. In the case of the second information request, MKB Bank provided only limited information to the data subject. Further, the NAIH also established that MKB Bank's privacy policy included only general information in relation to data processing, stating that MKB Bank processes personal data according to the provisions of the Privacy Act. Based on the above, the NAIH established that MKB Bank failed to fulfil the requirement of providing information in relation to data processing. <u>MKB Bank's liability as data controller</u> The NAIH established that MKB Bank as the data controller is liable for any act carried out by the employees of MKB Bank. Therefore, MKB Bank is liable for the inadequate information provided to the data subject by MKB Bank's employees.	The NAIH imposed a fine of HUF 500,000 (approx. EUR 1,666) on MKB Bank. Further, the NAIH ordered MKB Bank to fulfil the following obligations: – publish this decision on its website; – inform the NAIH within 30 days of all actions taken. The reason for the amount of fine imposed was that MKB Bank twice failed to provide information on data processing upon explicit request of the person whose personal data is the subject of data processing. Further, the NAIH intended to ensure special prevention and prevent MKB Bank from committing a similar infringement. The NAIH also intended to force MKB Bank to create a lawful practice in relation to providing information on data processing.
November	**Weltimmo S.R.O.**	Weltimmo made property ads available on the websites	The NAIH imposed a fine of HUF 8,500,000 (approx.

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
2016	("**Weltimmo**")	www.ingatlanbazar.com; www.ingatlandepo.com; and www.ingatlanbazar.net. The language of the websites was Hungarian (there was no possibility to change the language of the websites). Data subjects could freely publish their property ads after registration. However, after 30 days a certain fee was to be paid for publishing property ads. The NAIH received many complaints, according to which data subjects could not delete their registration and their property ads from the website, and they also could not contact Weltimmo. Some complainants also claimed that they could not log into their account created after registration. After 30 days the data subject received payment notification without any date, signature or stamp on it. Jurisdiction The NAIH established that Weltimmo falls under the Hungarian jurisdiction as only Hungarian property ads were available on the websites www.ingatlanbazar.com and www.ingatlandepo.com. Furthermore, the language of the websites was Hungarian, and they targeted users residing in Hungary. This was also confirmed by the CJEU in Weltimmo v. NAIH [the Hungarian Data Protection Authority] (C-230/14), please click here to read more. Property ads are considered as personal data The NAIH established that property ads should be considered as personal data even if they do not directly include data that would identify data subjects. Based on the NAIH decision, property ads should be considered as personal data as they can be linked to data subjects. (Data subjects provided personal data when they registered.) Infringement of rights of data subjects, obligation to delete personal data The NAIH established that Weltimmo failed to provide adequate information to data subjects in relation to data processing. The privacy policy available on www.ingatlanbazar.com did not include any information on the legal basis or the purpose of data processing, and did not specify until when personal data would be processed.	EUR 28,333) on Weltimmo. Further, the NAIH ordered Weltimmo to fulfil the following obligation: – to delete all property ads which are unlawfully processed in the archive database of the websites www.ingatlanbazar.com and www.ingatlandepo.com. The reason for the amount of the fine imposed was that Weltimmo infringed the rights of individuals to request deletion and information in relation to data processing. Further, Weltimmo infringed the principles of data protection when it did not specify the purpose and the legal basis of data processing. Furthermore, these infringements affected many individuals, who suffered a grave violation of their privacy (vis-à-vis the provisions of the Privacy Act). Finally, the infringing entity made a significant profit through such illicit practice. The NAIH considered favourably that Weltimmo positively changed its practice in relation to the deletion of personal data.

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
		Further, the privacy policy only referred to the fact that Weltimmo might publish the property ads on other websites belonging to Weltimmo; however it did not specify these websites. The NAIH established that Weltimmo failed to delete property ads being considered as personal data, despite the fact that data subjects requested to do so.	
November 2016	**Hungarian branch office of Cofidis** ("**Cofidis**")	Cofidis keeps records related to loans granted by Cofidis solely with the purpose of monitoring, controlling loans and debt recovery. Cofidis does not carry out overdue debt collection in the interests of other entities. Cofidis partly outsources activities related to debt recovery. Cofidis only contacts clients personally and/or in written (via post and in e-mail) and/or oral (via phone) form. In case of third persons (non-clients), Cofidis used to call third persons in order to obtain more details on clients; however, Cofidis stopped this "neighbouring" practice on 1 October 2014. Cofidis continuously reviews its database and uncovers data which are unlawfully processed. The Hungarian DPA (the "**NAIH**") received a complaint according to which Cofidis called and sent e-mail to third persons, usually neighbours of customers, in order to obtain more details on the complainant (client). The NAIH established that Cofidis failed to provide information related to data processing (e.g., legal basis of data processing, data retention period). The NAIH established that Cofidis conducted unfair practice when it tried to obtain and collect more data in relation to its clients from third persons (non-clients); Cofidis did not meet the requirement of obtaining the consent to such data processing; and Cofidis infringed the principle of purpose limitation.	The NAIH imposed a fine of HUF 1,000,000 (approx. EUR 3,333) on Cofidis. Further, the NAIH ordered the infringing company to fulfil the following obligations: – delete all personal data which lack adequate basis for legal processing (person who is not declared debtor). Deletion should be carried out in a verifiable manner by keeping relevant records at database level; – amend its practice to provide adequate information to data subjects; – publish this decision on its website by uncovering any confidential information included. The reason for the amount of fine imposed was that the infringements affected 96,070 clients and 245 third persons, and Cofidis committed the infringing activities continuously. The NAIH also took into account the size and market position of the infringing entity. The NAIH considered the following as a significant aggravating circumstance: - Cofidis stopped the unlawfully used "neighbouring"

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
			practice. The NAIH considered the following as mitigating circumstance: - Cofidis co-operated with the NAIH; - The number of third persons affected by the infringements is not significant compared to the number of clients. With this decision the NAIH intended to protect the legal interests of data subjects; therefore it ordered Cofidis to publish this decision on its website.

* Note that the Hungarian DPA usually does not publish the name of the infringing entity.

Italy

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed

[1] This table has been completed the most important cases examined in recent months by the Garante, without making reference to the several, as well as usual, claims made having regard to the exercise of the rights of the data subjects filed against banks and credit information companies.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
May 2017	WhatsApp Inc.	WhatsApp induced the users of its app to fully accept the new Terms of Use, in particular the sharing of their data with Facebook for product and marketing purposes. Those users who were already using WhatsApp at the time of the amendments to the Terms (25 August 2016) were given the possibility to partially accept the new Terms of Use, as well as to decide whether to share the information related to their WhatsApp account with Facebook or not. The Initial message invited the users to accept the new terms within 30 days to continue using the app; those users who did not accepted soon were invited to accept the new terms until the expiration of the 30 days otherwise they would have been prevented from any further use of the app after the 30 days term. The message also clarified that if the user did not intend to accept these new terms, he/she would be required to stop using the service. In to the case of both acceptance and refusal, the user was only offered the option to click on a button labeled “Accept”.	The Italian Antitrust Authority issued a fine of 3 million euro to WhatsApp Inc. for breach of the Consumer Code, citing unfair business practices that made consumers believe that the use of the app would have been impossible otherwise. Within the messages and at the end portion where the users were invited to learn more on the key amendments to WhatsApp terms and privacy policy, there were links corresponding to a landing page with a pre-flagged checkbox "*Share the info on my WhatsApp account with Facebook to enhance my experience with Facebook ads and products. Your chat and phone number will not be shared with Facebook*." The opt-in to the data sharing by default and the actual difficulty of exercising the option to not share the data with Facebook also contributed to the finding. Although the decision does not focus on data protection compliance issues, it strictly relates to modalities of issuing the notice and obtaining valid consent for sharing personal data with third parties.
May 2017	Wind Tre S.P.A. ("**Wind**")	Wind occurred a security breach incident involving more than 5118 customers (breach of personal data with the consequence of unlawful dissemination of customers' access credentials). Wind, with the collaboration of the third-party service provider, informed the Italian DPA and 402 of all customers involved in the breach immediately (the day after the incident occurred). To those customers, Wind - by several verifications - funded unauthorized access to their personal website. After the breach, Wind has blocked access to its web system and has adopted an automatic change of all 5118 passwords. Wind has in place a data breach internal procedure.	Italian Data Protection Authority ordered Wind to inform all the customers involved in the breach (except for 402 customers already informed), within 15 days from the receipt of the DPA decision. In addition Wind has to inform customers with all the details of Attachment II of the European Regulation 611/2013.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
April 2017	Tarì Scpa ("Tarì")	Tarì filed an ad authorization request before the DPA in order to obtain permission to retain the video surveillance images and data registered by the biometric control access system for 30 days, instead of 24 hours/ 1 week usually allowed by the Italian Data Protection legislation and general decisions of the DPA. Tari is a Goldsmith Centre, and it submitted its request based on objective reasons of security.	DPA authorized Tarì to retain the data and images up to 30 days, provided that Tarì complies with law n.300/1970 (Workers Statute of Rights).
February 2017	Yahoo!Italia Srl, Yahoo!Emea Limited	An Italian resident sought the removal of links to a US website reporting news of an old judicial matter from Yahoo!'s search engine. The news in question was outdated: the offence had been downgraded to a minor infraction, and the whole case dropped. The applicant had already addressed Yahoo! directly with the request, receiving an express rejection from the Company.	The DPA ordered Yahoo! Emea Limited to remove all links to the content at issue, enforcing the applicant's right to be forgotten against information that was "out of date". A similar principle was stated by the Court of Milan on 5th of January 2017 (decision no.12623).
February 2017	Sigue Global Service LTD and other companies in the sector of money transfer (Yume srl; Marc1 srl; Sirama srl; Euro Comunication System Srl) - all together "Company"	"Company" circumvented anti-money laundering laws, fractioning money transfers so that they were below the threshold of relevance for anti-money laws, and attributing the transfer to thousands of unaware customers whose personal data was unlawfully processed (particularly data of dead people and not -signatory party, whose data were collected using a copy of their Identity Card). This privacy breach related to data processing without the data subjects' consent.	Italian DPA fined the Company - that collected and transferred sums of money in China to Chinese entrepreneurs - a total amount of 11 million euro for breach of data protection laws (violation of articles 161, comma 2-bis and 164bis, comma 2 of Italian Privacy Code). More specifically the DPA has sanctioned: - an English company SIGUE GLOBAL SERVICE LTD for 5.880.000 euro; - an Italian company YUME SRL for 1.590.000 euro; - an Italian company SIRAMA SRL for 1.430.000 euro; - an Italian company EURO COMUNICATION SYSTEM SRL for 1.260.000 euro; - an Italian company MARC1 SRL for 850,000 euro.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
January 2017	Globo Vigilanza srl ("Globo")	Globo activated a localization system (innovative tracking system), using a GPS system and phone cards. This system was provided to employees involved with night video surveillance services, without provide employees with a complete and adequate privacy notice.	Italian DPA fined Globo an amount of 12.000 euro by way of a reduced pecuniary administrative sanction for failure to provide adequate privacy notice to its employees (art. 161 of the Italian Privacy Code).
January 2017	La Medico S.r.l	The Italian Data Protection Authority fined a nursing home for the omitted notification of the processing of sensitive data, with administrative fines of 40.000 euro. La medico Srl appealed the DPA decision.	The Italian Supreme Court (II Civil Section n. 188) confirmed the fines of 40.o00 euro, pointing out that the hospitals and clinics have to notify the DPA of the processing of sensitive data.
December 2016	Planetel S.R.L. ("Planetel")	Planetel, an Italian Company in the sector of telecommunication, adopted and provided to two employees with the same access credentials for the database SQL. In addition Planetel used a seven characters password instead of eight characters, as prescribed by the Italian Privacy Code. Planetel kept and archived telephone data traffic records in it server and area with unlimited access and for a period of more than 24 months (instead of the period of up to 24 months established by the Italian Privacy Code).	The Italian DPA fined Planetel 30.000,00 euro by way of a reduced pecuniary administrative sanction for failure to adopt adequate security measures, including the physical and remote security measures of area/ server where data are archived and violation of the lawful retention period (article 162 comma 2-bis with relation to articles 33, 17 and 132 comma 1 of the Italian Privacy Code).
December 2016	Aon S.P.A. ("Aon")	AON processed personal data contained in corporate e-mails and corporate device, such as blackberry (provided to employees) after the end of the employment relationship. The internal procedure governed the IT security system required to maintain mailboxes active for a period of up to six months after the end of the work relationship. In addition, the policy for data retention allowed 10 years on corporate servers (including extra EU countries) for both external data and the content of electronic communication (including communication exchanged using mobile devices). AON did not provide employees with an adequate, complete and clear privacy notice on the processing of their personal data, or a clear policy on the use of company's tools and devices.	On the basis of a complaint by a former AON employee, Italian DPA has declared unlawful the processing of the e-mail of employees and former employees due the violation of articles 3, 11 [comma 1, letter a)-d)-e)],13, 23 and 24, 113 and 114 of the Italian Privacy Code. Therefore, the DPA has prohibited the further processing of such data. Moreover, they have declared unlawful the processing of the data performed by mobile devices due the violation of articles 3, 11 [comma 1, letter a)-d)-e)], 13, 113 and 114 of the Italian Privacy Code, prohibiting any further processing of these data. In both case the employer could retain data with the civil/criminal purpose of protecting rights before a court, in compliance with article 160, comma 6 of the Italian Privacy Code.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
			The DPA reached such a conclusion by balancing between the interests of the employer in accessing the necessary information to safeguard efficient activities management, and the obligation to respect the confidentiality of their employees and third parties. The employer - while having the right to verify both job performance and proper use of tools and devices by the employees- must still respect their freedom and dignity. Therefore, without a clear and precise policy about how to use the company's tools and devices, as well as the checks that are carried out, employees are left unaware of which forms of communication can be regarded as confidential. A 10 years retention policy did not comply with the principles of necessity and proportionality set out in the Privacy Code, unless the employer provides specific reasons which make retention mandatory; in this case, circumstances did not appear commensurate with the effective needs of the company to manage e-mail services, including security requirements. In addition, a systematic collection of employees' electronic communications with a retention period of ten-years would allow companies to exercise the control of employees' activities violating article 4 of Workers Statute of Rights. The DPA also provides guidance on steps that have to be respected by an employer to close email accounts. In particular: before removing an account it is necessary to deactivate it while simultaneously implementing automatic systems which inform third parties and provide them with an alternative email address related to the professional activity of the former employee. Companies can collect data contained in electronic communication provided that they have previously informed employees about the means of data collection and about the time the account will remain active after the expiration of work relationship and the retention period (in compliance

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
			with Italian Privacy Code principles). DPA also pointed out that providing an automatic reply message which provides an alert about the account closing process and invites to forward communications to another valid email address, does not comply with the rules laid down by the Privacy Code. Same principles were issued by the Supreme Court (Civil Section- Labour) on 3rd of November 2016 (decision no. 22313). The Supreme Court pointed out that an employer has the right to verify the exact fulfillment of both job performance expectations and the proper use of tools and devices by the employees, but must respect their freedom and dignity while remaining in compliance with the principles set out by Privacy Code (art.11 comma 1 – lawfully, fairly and consistent with the scope for which data has been collected).
December 2016	Kiron Partener S.P.A. ("Kiron")	Kiron, an Italian company in the financial brokerage services sector and belonging to the group of Tecnocasa Holding s.p.a., has filed an authorization request before the Italian Data Protection Authority in order to obtain permission to retain data of its customers on its CRM for a period of 20 years instead of the 12/24 months allowed by the general decision of DPA of February 2005; this data would be held for the purposes of marketing and profiling activity. The retention period is strictly related to the business services provided by Kiron.	The DPA authorized Kiron to retain data for profiling and marketing activities for a period of 10 years, provided that at the expiration of the period the data would be automatically deleted or anonymized. The DPA has also stated that the privacy notices have to contain a clear indication of the type of processing and personal data collected for marketing and profiling purposes, and must also mention the voluntary nature of providing such data. This information has to be indicated in a separate section of the privacy notice.
December 2016	Furla S.P.A. ("Furla")	Furla filed an authorization request before the Italian Data Protection Authority in order to obtain permission to retain data of its customer on its new CRM (name, surname, date of birth, nationality, address, phone number, e-mail, details on their purchase, hobby, occupation, etc.) also for marketing (including market research activity) and profiling activity for a period of 10/7 years instead of the 12/24 months allowed by the general decision of DPA of February 2005. Customers' data can also be shared with other entities of Furla group	The DPA authorized Furla to retain data for profiling and marketing activities for a period of 7 years, provided that at the expiration of the period the data would be automatically deleted or anonymized. The DPA has also stated that the privacy notices have to contain all details about the Data Controller and the retention period.

Date	Infringing entity	Details of infringement[1]	Sanction(s) imposed
		(including those extra EU) provided that the European standard contractual clauses are in place.	
November 2016	Mevaluate Holding Ltd and Mevaluate Italia Srl and Associazione Mevaluate Onlus	An Italian company submitted some observations to the Italian Data Protection Authority in order to implement a web platform and electronic database that would rate the reputation of companies and individuals (the "Database"). Individuals would voluntarily submit their data (including sensitive and judicial data) into the Database. The Database would then collect and process both those data and other individuals' information, using an algorithm to objectively measure and rate the reliability of those individuals and companies.	Italian DPA under article 154, comma 1 letter d), has prohibited Associazione Mevaluate Onlus any processing of personal data using the Database due the non-compliance and violation of the Italian Privacy Code (articles 2,3,11,13,23, 24 and 26). The DPA, among others, has considered that the "reputational rating" was likely to negatively influence the lives of a large number of data subjects, affecting the dignity of the individuals.
October 2016	Wind Telecomunicazioni S.p.A. ("**Wind**")	Wind carried out a mass text-message campaign designed to persuade its customers (both new customers and those already registered in Wind's database) to give their consent to receive promotional messages, particularly those customers who have already denied their consent to receive promotional messages (via the web site portal).	On the basis of the claims made by several users, Italian DPA ordered Wind to immediately cease the processing of personal data without the explicit consent of the user for this type of campaign,. In addition the DPA required Wind to record into its system the right to oppose to the processing exercised by the user within 15 days from the users' request. The DPA reserved its right to verify the existence of the conditions to apply the administrative fines.

The Netherlands

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
May 2017	Facebook	After having conducted a large-scale investigation into the processing of data of over 9.6 million Dutch Facebook users, the DPA reported on 16 May 2017 that Facebook has violated data protection laws. The violations consisted, among others, of Facebook having insufficiently informed its users on its data processing activities. Moreover, Facebook has, without explicit consent, used users' data on sexual preferences for targeted advertising purposes.	After the investigation, Facebook has ceased to using data on sexual preferences for targeted advertising purposes. The DPA is currently assessing whether the other violations have also ceased. If the DPA finds this is not the case, it can impose sanctions on Facebook. Dutch press release: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-facebook-handelt-strijd-met-de-privacywetgeving
May 2017	Abrona	Abrona, a Christian organisation which provides services to people suffering from mental handicaps, processes data concerning the health of its incapacitated employees: it lists the cause and nature – physical or psychological – of the illness. In 2016, the DPA found that it is not allowed to process these sensitive data, as this is not necessary to make a relevant assessment of either future payments or the data subject's future activities.	The DPA has imposed upon Abrona a charge under penalty payment to end the infringements within a period of two months. On 4 May 2017 the DPA reported Abrona has ended all violations. No sanctions have been imposed. Dutch press release: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-abrona-beeindigt-overtredingen-met-gegevens-zieke-werknemers-0
May 2017	Municipality of Arnhem	The municipality Arnhem processes data of its citizens with regard to waste collection. The DPA has concluded that the data processing is not necessary for the municipality to fulfil its public task, and processing this data constitutes a violation.	Arnhem has taken measures to end the infringement: as of 2018, a new system will be put into place. Under the new regime, citizens will pay differentiated tariffs for their waste collection, depending on the amount of waste a citizen produces for collection. To determine a citizen's tariff (and therefore to fulfil its public task, it will be necessary for Arnhem to process personal data. The DPA has refrained from further enforcement measures. Dutch press release: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-gemeente-arnhem-past-afvalsysteem-aan
April 2017	Bluetrace	Bluetrace employs wifi tracking in numerous city centres and shopping malls to map numbers of visitors. In 2015, the DPA concluded that Bluetrace violated data protection regulations: it did not offer adequate (or in some cases, any) information on the occurrence of the	In first instance, Bluetrace took measures to end the infringements, which were found insufficient by the DPA. For example, Bluetrace still offered inadequate information to data subjects. Therefore, on 1 September 2016, the DPA imposed on Bluetrace a charge under penalty payment in order to urge Bluetrace to end the violations. On 20 April 2017 the DPA reported that Bluetrace ended wifi tracking in and around

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
		data processing, stored the collected data for too long and did not offer an opt-out to residents of the area.	stores; therefore, the DPA was satisfied the infringements had been ended. No penalties were imposed. Dutch press release: https://autoriteitpersoonsgegevens.nl/nl/nieuws/bluetrace-be%C3%ABindigt-overtredingen-wifi-tracking-na-optreden-ap

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
February 2017	Uniper	Uniper is a German company which processes medical data of its employees. Uniper asks for consent of its employees; however, if an employee refuses, he is required to be interviewed by his supervisor and might have to switch positions in the company. The DPA concluded that, although Uniper asks for consent, this consent cannot be freely given, as an employee possibly faces severe consequences if he refuses.	Uniper changed its refusal policy and no longer processes medical data of its employees. No sanctions were imposed. Dutch press release: https://autoriteitpersoonsgegevens.nl/nl/nieuws/uniper-trekt-alcohol-en-drugscontrolebeleid-na-onderzoek-ap
February 2017	The National Police	The DPA concluded that the Dutch Police take insufficient measures to ensure the adequacy of data enshrined in the Schengen Information System II (SIS II). The DPA stresses the importance of adequate data, as incomplete or inaccurate information can have severe consequences for people leaving or entering the Schengen zone.	The DPA has urged the Police to end the infringements. If the Police fail to do so, the DPA will impose sanctions. As of today, it is unclear whether the Police have commenced taking measures. Dutch press release: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-politie-heeft-onvoldoende-zicht-op-signaleringen-schengenlanden
February 2017	StemWijzer.nl	StemWijzer.nl is a website which offers users a series of questions, on the basis of which their political preferences are assessed. StemWijzer therefore processes sensitive data. The DPA found that StemWijzer faced several security threats. Moreover, StemWijzer used cookies without having obtained the consent of its users.	The DPA urged StemWijzer.nl to improve its security and to change its cookies policy. The DPA will continue to monitor the behaviour of StemWijzer.nl. As of now, no sanctions have yet been imposed. Dutch press release: https://autoriteitpersoonsgegevens.nl/nl/nieuws/toezichthouders-acm-en-ap-treden-op-tegen-stemwijzernl
November 2016	IND (Dutch Immigration and Naturalisation Service) and the Royal	Both institutions make use of the Schengen Information System II (SIS II) to process personal data of people entering or leaving the Schengen zone. The DPA concluded on 30 November 2014, with regard to the Royal Marechaussee, that it had taken insufficient security measures: for example, there was a no authorisation procedure present to access the system. As	On 22 November 2016, the DPA concluded that both the IND and the Royal Marechaussee had ended their respective infringements. The Marechaussee sufficiently improved its security measures, and the IND adjusted incomplete and inaccurate data. Dutch press release: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-koninklijke-marechaussee-en-

Date	Infringing entity*	Details of infringement	Sanction(s) imposed
	Netherlands Marechaussee	to the IND, the DPA found that it processed incomplete or inaccurate data.	ind-be%C3%ABindigen-overtredingen-sis
November 2016	WhatsApp	The DPA had ordered WhatsApp to designate a representative in the Netherlands pursuant to Article 4(2) of the Data Protection Directive. WhatsApp opposed this decision and commenced legal proceedings before the District Court of The Hague. The Court sided with the DPA.	A charge under penalty payment had been imposed by the DPA prior to commencement of the legal proceedings. However, this charge was suspended after the start of legal proceedings until judgment of the District Court was rendered. It is currently unclear whether either party has taken any subsequent steps. Judgment (in Dutch): https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2016:14088
November 2016	Nike	In its 'Nike+ Running app', Nike processes data concerning the health of its users. By analysing data collected over several months, Nike is able to make an assessment of a user's health. The DPA found on 10 November 2015 that Nike infringed data protection regulation: users had not given their explicit consent for the processing of these data and the data were stored for a disproportionately long time.	Nike has taken measures to end the infringements: in the new version of its Running app, Nike asks for explicit consent and offers better information regarding the processing of users' data. Moreover, after 13 months of inactivity, users' data are encrypted – only the user has access to the data, until they are deleted after 4 more years of inactivity. No sanctions were imposed. Dutch press release: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-nike-be%C3%ABindigt-overtredingen-hardloop-app

Poland

Date	Infringing entity	Details of infringement	Sanction(s) imposed
March 2017 (II SA/Wa 779/16)	Telecommunication service providers	The Inspector General for Personal Data Protection ("**GIODO**") has recently considered unlawful the practices of telecommunication service providers ("**TSP**s"), which have asked clients to provide a copy of their ID, driving licence or other documents with an image. Providing a copy of an ID by the client or asking the client to give his or her consent to copy the client's ID by the TSP's representative was	As a result of coordinated inspections in TSPs, GIODO issued several decisions in which it prohibited the above practices, and ordered deleting collected data in the above manner. GIODO's decisions have been challenged by TSPs,

Date	Infringing entity	Details of infringement	Sanction(s) imposed
		in many cases a prerequisite for concluding a contract on provision of telecommunication services, leading to excessive processing of the client's personal data, including: image, height, eye colour, permanent residential address, driving license number, driving license category, date of issuance and expiration date of the driving license.	however the Regional Administrative Court in Warsaw in the judgments of 18 February 2016 (case No. II SA/Wa 1655/15) and 28 March 2017 (case No. II SA/Wa 779/16) dismissed the complaints and upheld GIODO's decisions. Case No. II SA/Wa 779/16 is now being considered by the Supreme Administrative Court.
March 2017 (II SA/Ld 27/17)	The District Construction Supervision Inspector ("**PINB**")	On 9 March 2016, an individual requested PINB to disclose information on persons or entities to which PINB commissioned drafting legal opinions on matters related to PINB's activity acting in the capacity of a public authority. The individual acted under the legal basis provided under the Act on the Access to Public Information. It turned out that PINB's contractors were natural persons conducting individual business activity (sole traders). PINB refused to disclose their first names, last names and business names, and cited the Personal Data Protection Act as the legal basis prohibiting public disclosure of personal data of natural persons. PINB stated that as long as the information on the invoice issued with its identification number, date or amount payable is not restricted, the personal data of the issuing entity should not be disclosed, even if the public authority paid the contractor with public money. Moreover, according to PINB, these data constitute the personal interest of a natural person, referred to in Art. 23 of the Civil Code, which should be protected.	The Regional Administrative Court in Warsaw revoked PINB's decision and requested PINB to disclose the names of the natural persons to whom PINB commissioned legal services. The court stated that the right to public information is subject to restrictions, such as the privacy of a natural person, or the secrecy of an entrepreneur. Nevertheless, in this case we do not deal with the privacy of an individual, because the entity performing the service to the public authority and who issued the invoice is a sole trader. The sole trader is protected by trade secrets only, which extends to publicly available technical, technological or organisational information, or other information of economic value for which the entrepreneur has taken the necessary steps to preserve their confidentiality.
January 2017 (II SA/Wa 1574/16)	Bank	One of the Bank's clients applied for a mortgage. In order to evaluate the client's creditworthiness the Bank asked the client to provide his personal data. Personal data requested by the Bank included: name, address, address for correspondence, business telephone number, private telephone number, date of birth, place of birth, marital status,	GIODO requested by the client imposed the obligation on the Bank to delete all of the client's personal data. The Bank appealed GIODO's decision to the however, the Regional Administrative Court in Warsaw upheld

Date	Infringing entity	Details of infringement	Sanction(s) imposed
		ID number, e-mail, income, expenses, information on possessed assets, and others. Despite the submitted application, the contract between the client and the Bank was not concluded. The client asked the Bank to delete his personal data and to return all submitted documents. The Bank refused to delete the data and claimed that it processes the client's personal data on the basis of legitimate interest to defend itself against the client's potential complaints and claims that may occur in the future, as well as potential criminal proceedings concerning unlawful processing of the client's personal data by the Bank. GIODO stated that if the Bank did not conclude any contract with the client, the legal basis for processing the client's personal data consisting of the necessity for the performance of a contract, or in order to take steps at the client's request prior to entering into a contract (article 23 section 1 item 3 of the Polish Data Protection Act) is no longer valid. In GIODO's opinion, the Bank cannot process the client's personal data, even for statistical purposes. GIODO considered processing personal data of the person who is no longer a client of the Bank as collecting data "for the future" / "just in case", and thus deemed such action unlawful.	GIODO's decision and shared GIODO's views on the case. The Bank appealed the decision and the case is now being considered by the Supreme Administrative Court.

Singapore

Date	Infringing entity	Details of infringement	Sanction(s) imposed
May 2017	Furnituremart.sg ("**Furnituremart**")	This case concerns the leak of the personal data of a customer of Furnituremart ("Affected Customer"), which was contained in an invoice. The Affected Customer had signed and returned an invoice to Furnituremart upon the delivery of goods. However, the returned invoice was subsequently put in a printer feed tray, and re-used as printing paper for another customer's invoice.	The PDPC eventually issued the following directions to Furnituremart: (i) To review its policy for the protection of personal data in relation to its order fulfilment process; (ii) To develop procedures to ensure effective implementation of its data protection policy; and

Date	Infringing entity	Details of infringement	Sanction(s) imposed
		Furnituremart was eventually found to have breached its protection obligations under the PDPA for the following reasons: • Furnituremart's data protection policy was formalised during the month that the data breach occurred and could have been formalised after the unauthorised disclosure took place. • There was no evidence to show that steps had actually been taken to implement such policy prior to the breach. Further, Furnituremart admitted that its staff had no training whatsoever regarding their data protection obligations.	To conduct training to ensure that its staff are aware of, and will comply with, the requirements of the PDPA when handling personal data.
May 2017	Asia-Pacific Star Private Limited ("**APS**")	APS, by way of subcontracting by SATS Ltd (parent company of APS), was engaged to provide ground handling services for Tiger Airways Singapore Pte Ltd. On 26 July 2016, an APS employee disposed of a partially-printed flight manifest in the rubbish bin in the gate hold room for flight TR2466 and reprinted the flight manifest in full. The partially-printed flight manifest contained passenger personal data and was accessible to the passengers and airport staff in the gate's hold room. The PDPC found APS to be in breach of its PDPA protection obligations as it relied solely on the administrative safeguards implemented by SATS, which applied to the organisations within the SATS Group, and did not implement additional safeguards to contextualise the group level policies to its ground operations. APS should also have provided customised training and regular refresher training for APS employees who routinely handled passengers' personal data.	The PDPC eventually directed APS to: (i) conduct a review of its procedure for proper disposal of personal data in its possession and/or control; (ii) introduce data protection policies that are contextualised and pertinent to the services provided by APS and functions performed by its staff; and (iii) include a programme for initial and refresher training on its implementation by the APS staff in the course of its operations.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
April 2017	National University of Singapore ("**NUS**")	In May 2016, a Google Sheets spread sheet containing the data of student volunteers for a freshman orientation camp was circulated beyond the initially intended group of student leaders. Subsequently, an unknown party changed the settings for the spread sheet to allow any user who possessed the URL link to access the spread sheet. This resulted in the personal data set being exposed to those who had access to the URL link, which may have extended to persons beyond NUS itself. The PDPC found NUS to be in breach of its protection obligations under the PDPA as it did not have in place any formalised training for the student leaders despite it being reasonably foreseeable that personal data would be handled by them.	The PDPC eventually directed NUS to: (i) within 120 days from the date of the Commission's directions: a. design training on personal data protection for student events and of the resulting interactions; b. make arrangements for such training to be mandatory for any student leader; and c. make other arrangements as would be reasonably required to meet the objectives in (a) and (b) above; and by no later than 14 days after the above action has been carried out, submit to the PDPC a written update providing details on the arrangements for the training.
April 2017	Tech Mahindra (Singapore) Pte Ltd ("**Tech Mahindra**")	Tech Mahindra, an IT vendor, was engaged by Singapore Telecommunications Limited ("SingTel") to manage ONEPASS – a single login service allowing SingTel's customers to use the same credentials to access different SingTel accounts. In an attempt to update the ONEPASS account of a SingTel customer ("Customer"), Tech Mahindra committed a coding error in the database script which led to 2.78 million other ONEPASS accounts being modified to reflect the Customer's personal data. The PDPC found Tech Mahindra to be in breach of its PDPA obligations as Tech Mahindra had: • failed to follow SingTel's instructions regarding the database script which, if followed, would have prevented the error; • failed to comply with SingTel's standard operating procedures when updating the ONEPASS database; and	The PDPC eventually directed Tech Mahindra to pay a financial penalty of S$10,000 for its breach.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
		failed to comply with its own internal security standard operating procedures.	
January 2017	Propnex Realty Pte Ltd ("**Propnex**")	Propnex had uploaded an internal Do Not Call list ("DNC List") on its Virtual Office System ("VO System"), which contained the personal data of 1765 individuals. This DNC List was subsequently found to be searchable and accessible to the public without authentication required, due to it being indexed by Google. The PDPC found Propnex to be in breach of its PDPA protection obligations for the following reasons: • Propnex was aware of a significant weakness in the VO System and recognised that sensitive documents should not be placed on it, but failed to address this weakness. • Propnex's approach towards protecting documents in the VO System was insufficient, and showed an incorrect or inadequate understanding of the security measure which they chose to implement. The corrective measures taken by Propnex after the data breach incident were only sufficient as an interim measure.	The PDPC directed Propnex to pay a financial penalty of S$10,000 for its breach of the PDPA.
January 2017	JP Pepperdine Group Pte. Ltd. ("**JP Pepperdine**")	JP Pepperdine is a restaurant operator in Singapore and had a membership programme with approximately 30,000 members as of December 2015. Upon investigating, the PDPC found that sensitive personal data of members of the membership programme were made publicly accessible through the membership webpage by (i) entering a randomly simulated membership number in the search facility on the Webpage, which would retrieve membership details associated with that account; or (ii) simply clicking on the “Search” button in the search facility without any search parameters, would randomly	The PDPC directed JP Pepperdine to pay a financial penalty of S$10,000 for its breach within 30 days of the PDPC's direction.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
		retrieve the details of a membership account. The PDPC found JP Pepperdine to be in breach of its protection obligations under the PDPA for the following reasons: • JP Pepperdine had failed to conduct a review of its system, which was implemented prior to the introduction of the PDPA only for internal and temporary purposes, so as to determine its weakness and vulnerabilities. • JP Pepperdine did not take any steps to detect and rectify the severe loophole in the webpage which allowed unauthorised access to personal data stored on the server. • JP Pepperdine did not implement any security or access controls to the webpage. It was unacceptable to allow for the use of the membership number assigned to each member to serve the functions of identification and authentication to access personal data, since the numbers were both assigned in running sequence and easy to deduce.	
December 2016	The Cellar Door Pte Ltd ("**Cellar Door**") Global Interactive Works Pte. Ltd. ("**GIW**")	Cellar Door was in the business of selling food and wine products and had a business website that was designed, developed, hosted and backed up by GIW. Cellar Door's customer database was also hosted on GIW's server. Around September 2014, the PDPC found unauthorised postings on a website known as "Pastebin", comprising of personal data of Cellar Door's customers on Cellar Door's website. Eventually, the PDPC found that Cellar Door and GIW, as a data intermediary for Cellar Door, had breached their protection obligations under the PDPA as they had (i) inadequate security policies and processes to protect the personal data; and (ii) failed to put in place an overall security to guard against intrusions, attacks or	The PDPC directed Cellar Door to: (i) within 60 days from the date of the Commission's direction: a. conduct a vulnerability scan of the Site; b. patch all vulnerabilities identified by such scan; (ii) submit to the PDPC within 14 days after the conduct of the abovementioned scan, a written update providing details on: a. the results of the scan; b. the measures that were taken by Cellar Door to patch all vulnerabilities identified by the vulnerability scan; and (iii) pay a financial penalty of S$5,000 within 30 days

Date	Infringing entity	Details of infringement	Sanction(s) imposed
		unauthorised access. Several gaps in security measures were highlighted, such as the lack of a server firewall, the leaving of unused ports open, the transfer of login credentials in clear and unencrypted text and a weak administrative password.	from the date of the PDPC's direction. Separately, the PDPC also directed GIW to pay a financial penalty of S$3,000 within 30 days from the date of the PDPC's direction.
November 2016	Smiling Orchid (S) Pte Ltd ("**Smiling Orchid**")	The complainant was a customer of Smiling Orchid, a food catering company, and had placed an order on Smiling Orchid's website. Subsequently, the complainant performed an internet search of his full name on www.yahoo.com.sg and among the search results was a URL link to a website containing details of the complainant's order, which included his personal data. The PDPC found Smiling Orchid to be in breach of its protection obligations under the PDPA as: (i) there was no clear designation of security responsibilities by Smiling Orchid; (ii) the investigations undertaken were poorly conducted; and (iii) the corrective actions undertaken were insufficient to address the problem with the system.	The PDPC directed for a financial penalty of S$3,000 to be imposed on Smiling Orchid. In addition the PDPC also directed that: (i) Smiling Orchid shall, within 120 days from the date of the Commission's direction: a. put in place the security arrangements for the new website to protect the personal data that was collected, or may be collected, by Smiling Orchid; b. conduct a web application vulnerability scan of the new website; and c. patch all vulnerabilities identified by such vulnerability scan; and by no later than 14 days after the above action has been carried out, submit to the PDPC a written update providing details on (i) the results of the vulnerability scan; and (ii) the measures that were taken by Smiling Orchid to patch all vulnerabilities identified by the vulnerability scan.

Spain[2]

Date	Infringing entity	Details of infringement	Sanction(s) imposed
February 2017	Liberbank S.A	On 17 September 2015, a letter from a natural person was filed before the Spanish Data Protection Agency ("**SDPA**"), claiming that Liberbank S.A. sent a burofax in which it claims a debt for the non-payment of a loan. The individual claimed that he had no relationship with this entity and that upon contacting with it, he has been informed that his national identification number did not match the one of the debtor. Notwithstanding, Liberbank S.A. did not specify the way in which they obtained the claimant's data to send the burofax. Liberbank S.A. stated that the address of the complainant was obtained from sources accessible to the public "Páginas Amarillas"(Spanish Phone book). The SDPA estimated that the conduct of Liberbank S.A. infringed article 6.1 of the Organic Law 15/1999, of December 13, on Data Protection (hereinafter, "**LOPD**" as per its Spanish initials), even though the data of the complainant's home was obtained through a public source, "Páginas Amarillas", it was then compared to the data in their own data base and without any sort of verification of identity they sent the burofax to the claimant demanding payment of a debt and warning that if he did not pay, he could be included in a debtors data file. Finally, the SDPA initiated a sanctioning procedure for the infringement of Article 6.1 of the LOPD, which states that the processing of personal data requires the unequivocal consent of the person concerned, except when the law states otherwise.	Processing personal data without having collected the data subject's consent is a serious infringement of the data protection legislation that, in this case, was subject to a fine of €50,000.

[2] Please note that the enforcement action for Spain is in overview only as the Spanish DPA is very active in this area.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
February 2017	Banco Bilbao Vizcaya Argentaria S.A.A ("**BBVA**")	On 8 September 2015, a letter from a natural person was filed before the SDPA, claiming that it was a customer of BBVA and that, on 22 June 2015, ISOTROL SA, sent him a document in pdf format for the fulfilment of the company's data processing obligations with his personal and financial data already completed. The claimant did not provide such company with his personal data, nor had he authorised his bank, BBVA, to communicate his data to this company. BBVA disclosed personal data of the complainant to third parties, which meant that the duty of secrecy imposed by Article 10 of the Data Protection Act was violated. This article provides that "the person responsible for the file and those who intervene at any stage of the processing of personal data are bound to the professional secrecy with respect to them and to the duty to keep them, obligations that will remain even after finalizing their relations with the owner of the file or, if applicable, with the person responsible for the same ".	Violating the duty of secrecy in this case, was subject to a fine of €50,000.

Date	Infringing entity	Details of infringement	Sanction(s) imposed
January 2017	Orange Espagne SAU ("**Orange**")	On 17 August 2015, a letter from an individual was filed before the SPDA requesting the erasure of his personal data due to the fact that his personal data had been included in a debtor file by Orange. On 28 June, the claimant was included in a debtor data file for an alleged debt of €62.96 with Orange. However, on 16 March, the complainant filed a complaint before the Spanish Telecommunications Secretary of State for improper billing and breach of contract by Orange. Although the aforementioned public body has not yet ruled on such claim, Orange decided to include his data in a debtors data file. On 11 July, the complainant sent the certified letter to Badexcug, (the company managing debtor data file) and the data controller requesting the exercise of the right of erasure, since there was no demand for payment until the resolution of the Secretary of State. After that, the complainant received the notification from the data controller denying the erasure of his data. Finally, the director of the SDPA sanctioned Orange, for the infringement of Article 4.3 in relation to 29.4 of the LOPD and 38.1.a) and c) of the RLOPD.	Infringing Article 4.3 is considered a serious infringement of the data protection legislation and the fine imposed was €50,000.

Sweden

Date	Infringing entity	Details of infringement	Sanction(s) imposed
May 2017	Midasplayer AB ("**Midasplayer**")	In response to information that Midasplayer registered information regarding its employees' sexual orientation and ethnic origin, the DPA decided to conduct an audit of Midasplayer's processing of its employees' personal data. According to Midasplayer, they collected and processed the information to improve diversity and equal treatment within the company. The processing was based on consent obtained from the employees. Under the PDA a data subject's consent for the processing of its personal data shall be voluntary, specific, informed and unambiguous. The DPA stated that obtaining consent in an employee-employer relationship could be of limited value since it is questionable whether the employees – given their subordinate position vis-à-vis the employer – are able to express a voluntary consent in relation to their employer's need to process their personal data. The DPA concluded that the consent collected from the employees for the processing did not fulfil the formal requirements for a valid consent under the PDA, since it could not be considered to be provided voluntary. Thus, the DPA found that Midasplayer processed personal data in breach of the PDA by processing sensitive personal data regarding its employees without a valid legal ground for the processing.	The DPA ordered Midasplayer to cease all processing of the relevant sensitive personal data.

May 2017	Google Inc. / Google Sweden AB ("**Google**")	In May 2014, the European Court of Justice ("**ECJ**") concluded that an individual may request that search engines, such as Google, delete search results that include the individual's name if the search results are inaccurate, inadequate, irrelevant, no longer relevant or excessive. This opportunity is sometimes referred to as the "right to be forgotten." After the ECJ judgment, thousands of persons have turned to Google and asked them to delete results of searches made on the basis of their names. Some of those who have not had their search results deleted have submitted complaints to the DPA. Out of these, the DPA selected thirteen complaints and analyzed these further. The DPA found that Google in five of the thirteen complaints processed personal data in breach of the PDA by not complying with the "right to be forgotten".	The DPA ordered Google to delete search results related to the five complaints so that such results are not shown when searches are made from Sweden. The DPA further ordered Google to delete search results shown by searching the data subject's name in Google's search engine when searches are made from other countries if it in the individual case can be considered as that the search results has such a specific connection to Sweden and to the data subject that they constitute an infringement of the data subject's personal integrity.
January 2017	Örebro University (the "**University**")	The DPA received a complaint from a parent with regard to the University's processing of personal data of a high school student in a research study (the "**Study**"). The DPA decided to, based on the complaint, conduct an audit of the University's processing of personal data in the Study. The DPA found that the University, due to the method for collecting personal data, collected survey responses for the Study comprising sensitive personal data of children whose parents had stated that the child should not participate in the Study. According to the DPA, the University therefore processed and was at risk of processing personal data/sensitive personal data in breach of the PDA by collecting more personal data than necessary for the Study.	The DPA ordered the University to cease the collecting and processing of survey responses for the Study comprising sensitive personal data of children whose parents had stated that the child should not participate in the Study.
December 2016	Statistics Sweden ("**Statistics**") (Sw. *Statistiska centralbyrån*)	The Swedish Data Protection Authority ("**DPA**") conducted an audit of the Statistics' processing of personal data in its survey "Hälsa Stockholm" (Eng. *Health Stockholm*). The DPA found that Statistics processed personal data in the survey "Hälsa Stockholm" in breach of the Swedish Personal Data Act (1998:204) ("**PDA**") by processing personal data for the survey without valid legal grounds for the processing.	The DPA ordered Statistics to cease the processing of personal data conducted in relation to the survey "Hälsa Stockholm."

United Kingdom

Date	Infringing entity	Details of infringement	Sanction(s) imposed
June 2017	Boomerang Video Ltd	Boomerang Video Ltd suffered a cyber-attack in December 2014. An investigation by the ICO found the Berkshire-based company failed to take basic steps to stop its website being attacked.	£60,000 fine imposed.
June 2017	MyHome Installations Ltd	The ICO received 169 complaints concerning the calls made by MyHome Installations Ltd to phone numbers listed on the Telephone Preference Service (TPS), the UK's official opt-out of telephone marketing register.	£50,000 fine imposed.
June 2017	WM Morrison Supermarkets Plc	Morrisons sent an e-mail to 236,651 (of which 130,671 were successfully received) individuals titled "Your account details" advising them that they had chosen not to receive marketing communications from Morrisons because they had opted out of Morrisons More card marketing. It invited them to change their preferences to start receiving money off coupons, extra More Points and latest news and provided directions on the steps to follow to opt back in to receive marketing.	£10,500 fine imposed.
June 2017	Gloucester City Council	The Council's IT staff identified a vulnerability in their IT systems in April 2014. They failed to take appropriate measures and then suffered a cyber-attack in July 2014.	£100,000 fine imposed.
May 2017	Basildon Borough Council	In July 2015, an administrator at the Council received a planning statement in support of a householder's application for proposed works in a green belt that contained sensitive personal data relating to a static traveller family. The administrator uploaded the planning application without redacting this sensitive personal information.	£150,000 fine imposed.

May 2017	Concept Car Credit Limited	Between 9 April 2015 and 5 March 2016, 66 complaints were made to the 7726 service, or direct to the Commissioner, about the receipt of unsolicited direct marketing text messages sent on behalf of Concept Car Credit Limited. The content of some of the text messages were as follows: “URGENT. Finance deals approved 4 you to drive your new car away today, no deposit and 100 cash back. CALL NOW 01204466400 or conceptcarcredit.co.uk OPT OUT: STOP”. “Looking 4 Car Finance, we can help. Up to Â£200 cash back, no deposit & drive away same day. Call 01204466400 or apply @ conceptcarcredit.co.uk OPT OUT; STOP”. “Urgent your approval 4 car finance expires today up to 200 cashback no deposit open until 8pm! Call 01204446400 or visit conceptcarcredit.co.uk OPT OUT; STOP”. Concept Car Credit Limited explained that it had obtained the data used to send the text messages from a number of third parties with whom they hold introducer agreements between 2012 and 2016, but was unable to provide sufficient evidence that the individuals to whom the text messages had been sent had consented to the receipt of those messages.	£40,000 fine imposed.

May 2017	Brighter Home Solutions Ltd	Between 4 January 2016 and 26 August 2016, the TPS received 160 complaints about Brighter Homes. The TPS, maintained by OFCOM at that time, referred all of those complaints to Brighter Homes and also notified the ICO. Brighter Homes did not respond to the TPS in relation to any of the complaints. Some of those individual subscribers complained that the calls were misleading because the callers gave the impression that they were calling from a local number and were misled into believing that they may have been contacted by Brighter Homes previously and agreed at that time to receive further calls in the future. The ICO found that between 4 January 2016 and 26 August 2016, Brighter Homes used a public telecommunications service for the purposes of making 187 unsolicited calls for direct marketing purposes to subscribers where the number allocated to the subscriber in respect of the called line was a number listed on the register of numbers kept by the Commissioner.	£50,000 fine imposed.
May 2017	Onecom Limited ("**Onecom**")	Between 26 October 2015 and 2 June 2016, 1050 complaints were made to the 7726 service, or direct to the Commissioner, about the receipt of unsolicited direct marketing text messages relating to mobile phone upgrades. The data used by Onecom for sending the marketing text messages had been obtained from various sources: (i) data acquired through the acquisition of other businesses; (ii) data obtained by Onecom from its own customers; and (iii) data obtained from third party data suppliers. Onecom could not provide any evidence to the Commissioner as to the source of the data used to send the 1050 text messages. Further, 7 Onecom was unable to provide evidence that it had consent to send those text messages or that it could rely on the 'soft opt-in'.	£100,000 fine imposed.

May 2017	Keurboom Communications Limited ("**Keurboom** ")	Between 29 April 2015 and 7 June 2016, the Commissioner received 1,036 complaints about Keurboom making automated marketing calls, mainly in relation to road traffic accidents and PPI claims. Some complainants had also received repeat calls and at unsocial hours. The ICO found that Keurboom had instigated 99,535,654 automated marketing calls to subscribers without their prior consent.	£400,000 fine imposed.
May 2017	Greater Manchester Police ("**GMP**")	In 2015, GMP sent three unencrypted DVD's to the NCA's Serious Crime Analysis Section by Recorded Delivery. The DVD's each contained a video of a police interview with victims discussing sensitive information in an on-going case. The DVDs were never received by the NCA's Serious Crime Analysis Section and have not been recovered to date. The ICO found that GMP failed to take appropriate organisational measures for ensuring that such an incident would not occur.	£120,000 fine imposed.
May 2017	Construction Materials Online Limited ("**CMO**")	CMO operated a website environment that enabled its customers to purchase building products online by entering their card details. Whilst card details were encrypted by CMO before being sent directly to an external payment system, there was a coding error in the login pages that CMO were unaware of. Such coding error was exploited by a cyber-attacker who obtained payment card details from the website for 669 users. The ICO found that CMO failed to take appropriate measures for ensuring that such an incident would not occur.	£55,000 fine imposed.
April 2017	Monevo Limited	Monevo Limited was found by the ICO to be responsible for sending 44,172 unsolicited marketing texts promoting loans.	£40,000 fine imposed.

April 2017	Great Ormand Street Hospital Children's Charity ("**GOSH**"); Battersea Dogs' and Cats' Home ("**BDCH**"); Cancer Research UK; Cancer Support UK; Macmillan Cancer Support; National Society for the Prevention of Cruelty to Children ("**NSPCC**"); Oxfam; The Guide Dogs for the Blind Association ("**GDBA**"); International Fund for Animal Welfare ("**IFAW**"); The Royal British Legion; and WWF-UK.	GOSH, Cancer Support UK, IFAW and WWF-UK shared records with each other, no matter what the cause between 2011 and 2015. Also between 2010 and 2016, GOSH, Cancer Research UK, Macmillan Cancer Support, NSPCC, GDBA, IFAW, The Royal British Legion and WWF-UK sent thousands of records per month to a wealth screening company. Further to this, GOSH, BDCH, Cancer Research UK, Macmillan Cancer Support, NSPCC, Oxfam, GDBA, IFAW, The Royal British Legion and WWF-UK approached third party companies to match email addresses and dates of birth to supporters.	GOSH was fined £11,000. BDCH was fined £9,000. Cancer Research UK was fined £16,000. Cancer Support UK was fined £16,000. Macmillan Cancer Support was fined £14,000. NSPCC was fined £12,000. Oxfam was fined £6,000. GDBA was fined £15,000. IFAW was fined £18,000. WWF-UK was fined £9,000.
March 2017	PRS Media Limited ("**PRS**")	Between 1 January 2016 and 17 May 2016, PRS used a public telecommunications service for the purposes of instigating the transmission of 4,357,453 unsolicited communications by means of electronic mail to individual subscribers. The ICO found that PRS did not have the correct consents for such marketing communications.	£140,000 fine imposed.
March 2017	Xternal Property Renovations Ltd ("**Xternal**")	Between 14 August 2015 and 11 April 2016, the Xternal used a public telecommunications service for the purposes of making 131 unsolicited calls for direct marketing purposes to subscribers where the number allocated to the subscriber in respect of the called line was a number listed on the register of numbers kept by the Commissioner.	£80,000 fine imposed.

March 2017	Flybe Limited	On 15 August 2016, Flybe Limited instigated the transmission of 3,333,940 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The ICO was satisfied that the appropriate consents had not been obtained.	£70,000 fine imposed.
March 2017	Honda Motor Europe Limited ("**Honda**")	Between 1 May 2016 and 22 August 2016, Honda instigated the transmission of 289,790 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The ICO found that Honda did not have the correct consents for such marketing communications.	£13,000 fine imposed.
March 2017	Norfolk County Council	A third party collected redundant furniture, including filing cabinets, from the Norfolk County Council offices in April 2014. Later that month a member of the public bought a filing cabinet and found sensitive information contained within it. ICO found that Norfolk County Council did not have the correct procedures in place to ensure against such an incident.	£60,000 fine imposed.
March 2017	Munee Hut LLP	Munee Hut LLP instructed a firm in Belize to send around 64,000 spam text messages promoting loans on its behalf without obtaining the appropriate consents from the recipients.	£20,000 fine imposed.
March 2017	Road Accident Consult Limited	Between 13 November 2014 and 9 June 2015 the Company instigated the transmission of 22,065,627 automated marketing calls to subscribers without their prior consent.	£270,000 fine imposed.
February 2017	HCA International Limited ("**HCA**")	HCA owns the private Lister Hospital in London. The hospital routinely sent unencrypted audio recording by email to a company in India for transcription. The recordings contained private consultations that took place with a doctor and patients wishing to undergo IVF treatment. Such recordings were subsequently able to be accessed via an internet search engine. The ICO found that HCA failed to take appropriate measures against unauthorised or unlawful processing.	£200,000 fine imposed.

February 2017	Digitonomy Limited ("**Digitonomy**")	Between 6 April 2015 and 29 February 2016, the Digitonomy used a public telecommunications service for the purposes of instigating the transmission of 5,238,653 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The ICO found that Digitonomy did not have the correct consents for such marketing communications.	£120,000 fine imposed.
February 2017	The Data Supply Company Limited ("**DSC**")	Between 19 June 2015 and 21 September 2015, 174 complaints were made to the 7726 service or direct to the Commissioner about the receipt of unsolicited direct marketing text messages about pay day loans. Following an investigation, the ICO established that the person responsible for sending those text messages had obtained its data from DSC. DSC had provided 580,302 records containing personal data.	£20,000 fine imposed.
January 2017	LAD Media Limited	Between 6 January 2016 and 10 March 2016, LAD Media Limited used a public telecommunications service for the purpose of instigating the transmission of 393,872 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The ICO found that LAD Media Limited did not have the correct consents for such marketing communications.	£50,000 fine imposed.
January 2017	IT Protect Limited	Between 6 April 2015 and 16 May 2016, IT Project Limited used a public telecommunications service for the purpose of making 157 unsolicited calls for direct marketing purposes to subscribers where the number allocated to the subscriber in respect of the called line was a number listed on the register of numbers kept by OFCOM. The ICO found that IT Project Limited did not have the correct consents for such marketing communications.	£40,000 fine imposed.

January 2017	Royal & Sun Alliance Insurance PLC ("**RSA**")	At some point between 18 May and 30 July 2015, a portable 'Network Attached Storage' device ("device") was taken offline and stolen by a member of staff or contractor who was permitted to access the data 4 server room ("DSR") in the RSA's premises. The device held personal data sets containing 59,592 customer names, addresses, bank account and sort code numbers and 20,000 customer names, addresses and credit card 'Primary Account Numbers'. It was password protected but not encrypted. The ICO found that RSA failed to take appropriate measures against unauthorised or unlawful processing.	£150,000 fine imposed.
December 2016	British Heart Foundation; The Royal Society for the Prevention of Cruelty to Animals ("**RSPCA**")	British Heart Foundation and RSPCA shared records with each other, no matter what the cause between 2011 and 2015. Also the British Heart Foundation and RSPCA sent thousands of records per month to a wealth screening company. Further to this, the British Heart Foundation and RSPCA approached third party companies to match email addresses and dates of birth to supporters.	British Heart Foundation was fined £18,000. RSPCA was fined £25,000.
November 2016	Oracle Insurance Brokers Limited	Between 5 May 2015 and 21 December 2015, Oracle Insurance Brokers Limited used a public telecommunications service for the purposes of instigating the transmission of 136,369 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The ICO found that Oracle Insurance Brokers Limited did not have the correct consents for such marketing communications.	£30,000 fine imposed.
November 2016	Silver City Tech Limited	Between 11 November 2015 and 17 December 2015, Silver City Tech Limited instigated the use, via third party affiliates, of a public telecommunications service for the purposes of transmitting 1,132,149 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The ICO found that Silver City Tech Limited did not have the correct consents for such marketing communications.	£100,000 fine imposed.

November 2016	Historical Society	An administrative officer working for the Historical Society left an unencrypted laptop at one of their premises. Those premises were broken into and the laptop was stolen. The ICO found that the Historical Society had failed to take appropriate measures against unauthorised or unlawful processing.	£500 fine imposed.
November 2016	Assist Law Limited	Between 29 April 2015 and 15 April 2016, Assist Law Limited used a public telecommunications service for the purposes of instigating the transmission of 99 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The ICO found that Assist Law Limited did not have the correct consents for such marketing communications.	£30,000 fine imposed.
November 2016	Nouveau Finance Limited	Between 1 August 2015 and 31 January 2016, Nouveau Finance Limited used a public telecommunications service for the purposes of instigating the transmission of 2.2 million unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The ICO found that Nouveau Finance Limited did not have the correct consents for such marketing communications.	£70,000 fine imposed.
October 2016	Rainbow UK Limited	Between 19 June 2015 and 21 September 2015, Rainbow UK Limited used a public telecommunications service for the purposes of instigating the transmission of 21,045 unsolicited communications by means of electronic mail to individual subscribers for the purposes of direct marketing. The ICO found that Rainbow UK Limited did not have the correct consents for such marketing communications.	£20,000 fine imposed.

October 2016	TalkTalk Telecom Group PLC	In 2009, TalkTalk acquired the UK operations of Tiscali. Between 15 and 21 October 2015, a cyber-attack exploited vulnerabilities in three of Tiscali's webpages that provided access to an underlying customer database. TalkTalk was unaware of such vulnerabilities. The ICO found that TalkTalk had not taken appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data.	£400,000 fine imposed.

Data protection news

China

Clarice Yue, Counsel, Michelle Chan, Partner, Bird & Bird, Hong Kong office, Sven-Michael Werner, Partner, Bird & Bird, Shanghai office & John Shi, Partner, Bird & Bird, Beijing office

Cyber Security Law Update: Critical Network Equipment and Dedicated Cyber Security Products Catalogue issued

The article is published here.

Cyber Security Law Update: Finalised Measures on Security Examination of Network Products and Network Services Issued!

The article is published here.

Cyber Security Law Update: Data localisation coming to China

The article is published here.

Cyber Security Law Update: Will Network Products and Network Services Pass the Test?

The article is published here.

Cyber Security Law Update: Critical Information Infrastructure in China – Any clarification?

The article is published here.

Cyber Security Law in China: At Long Last!

The article is published here.

Czech Republic

Andrea Jarolimkova, Associate & Marketa Krizakova, Associate, Bird & Bird, Prague office

Change in approach of the DPA to biometrics

In June 2017, the Czech DPA issued a short announcement concerning their approach to biometrics. To date, biometrics were governed by the Czech Data Protection Act and the Opinion No. 3/2009 of the Czech DPA. This Opinion practically divided systems with biometric data into systems that are treated such as systems processing standard personal data (usually templates) and systems processing sensitive data (usually raw biometrics) that need stricter protection. However, according to the DPA, the General Data Protection Regulation brings substantial change in the legal approach to this topic as the keeping of biometric templates and their processing in order to identify persons is considered to be the processing of a special category of personal data.

According to the DPA biometric technologies cannot fully replace other security solutions and they do not ensure higher security by themselves. Controllers using such systems have to consider proportionality of the particular solution and the risks connected to them (e.g. systems keeping databases of biometric templates) and they also have to appropriately combine biometric systems with other security measures. Prior to implementation as well as continuously afterwards, controllers have to consider the effectiveness of biometric systems and examine whether there are serious reasons justifying the installation and operation of such systems. The DPA already takes into account this approach when carrying out the inspections and is also planning to publish an updated opinion in the future.

Liability for sending unsolicited commercial communications

In June 2017, the DPA issued a short statement saying that it is not only distributors of unsolicited commercial communications that can be held liable for the distribution of such communications. Aside from the distributor, the DPA will also prosecute those subjects who profit from the commercial communication that was sent and who initiated such communication (email campaign), typically upon instruction, order, contract or other similar acts. It is not possible for an entity to be released from the liability for distributing commercial communications by mere transfer to the distributor through a concluded agreement. The DPA emphasises that it is possible to distribute commercial communications via email or SMS only in compliance with the statutory conditions. One of these conditions is the consent of an addressee of commercial communication, unless it is a customer. The consent has to be provable and the burden of proof lies on the distributor.

Denmark

Amalie Langebaek, Associate, Bird & Bird, Copenhagen office

General Data Protection Regulation Report

On 24 May 2017 the Danish Ministry of Justice issued its report on the General Data Protection Regulation ("**GDPR**"). The report reflects upon and clarifies the Danish view on the areas of the GDPR that are left to the Member States to decide. However, a lot of questions are still unanswered and will instead be left to be clarified in a future Danish bill on the GDPR.

Data protection legislation comes into force in Greenland

On December 2016 the Danish legislation on processing of personal data: *Persondataloven* became effective in Greenland.

Finland

Karoliina Kallasvuo, Associate, Maria Aholainen, Associate, Tobias Bräutigam, Counsel, & Sakari Halonen, Partner, Bird & Bird, Helsinki office

Ombudsman given the right to order Google Search to remove URL addresses

On 8 December 2016, the Administrative Court of Helsinki gave a decision stating that the Finnish Data Protection Ombudsman had the right to order two URL addresses to be removed from Google Search, when searches were performed with the name of a certain individual. The Administrative Court stated that respective search results were unnecessary for the purposes of processing the controller's personal data. The respective personal data (behind URL addresses) not only described a homicide committed by the individual and said individual's imprisonment, but also information concerning that individual's health. In its decision, the Administrative Court did not prohibit to link said URL addresses to other searches than those that were performed with the individual's name. No sanctions were imposed.

Religious group's role as data controller referred to CJEU

On 28 December 2016, the Finnish Supreme Administrative Court referred to the EU Court of Justice for a preliminary ruling a question about personal data processing in relation to the preaching work of Jehovah´s witnesses. The questions related to whether personal data processing of this religious group is in the scope of the Data Protection Directive, and whether the religious group should be interpreted to be data controller of personal data collected by individual members of the religious group.

Consultation on four legislative proposals

On 19 April 2017, four legislative proposals were given in Finland for legislation on civilian and military intelligence, and on different aspects of intelligence powers and oversight. The next step in preparation is a consultation process. It is expected that formal government proposals on intelligence legislation will be submitted to the Finnish Parliament during fall 2017. At present, Finland does not have comprehensive legislation regarding network surveillance without a concrete suspicion of a criminal activity, which makes Finland an exception within the European Union. As the proposed legislation would require an amendment to the Finnish Constitution, the progress of the proposed legislation is highly dependent on the political state of affairs.

Germany

Dr. Natallia Karniyevich, Associate & Lennart Schüßler, Partner, Bird & Bird, Dusseldorf office

Germany is the first EU Member State to enact new Data Protection Act to align with the GDPR

This article is published here.

Italy

Debora Stella, Associate, Bird & Bird, Milan office

New rules for call centres located in non-EU countries

According to the new law no. 232 of December 2016, the Italian DPA, starting on 1st of January 2017 collaborates with Italian Ministry of Economic Development in order to verify if all the companies using call centres in non-EU countries are compliant with the new terms of the law. New rules on call centres require any call centre to clarify on the call from which country the operator is answering the call and to register within the ROC (Register of Communication Operator) the Italian phone numbers used to offer the call centre service.

In addition, if the call centre is based outside the EU the company that outsources the call centre services to a third party outside the EU must also (i) register the service and telephone numbers with the Italian Ministry of the Economic Development; (ii) communicate to the Italian Ministry of Labour whether or not there have been dismissals in any local branch in Italy as a consequence of this outsourcing; and (iii) communicate to the Italian DPA, by using a specific template, the transfer of data outside the EU. The fine in the case of omitted or late notifications of an administrative fine are from €10,000 to €150,000 respectively for each day of delay and for each omitted notification, in addition to any fines that might result from failure to comply with the Italian Data Protection Code (legislative decree 196/2003). Company (i.e. the Client) and the Service Provider are jointly and severally liable for any violation.

First Guide on the application of the General Data Protection Regulation

On April 2017, the DPA published on its website a first guide on the application of the GDPR. The DPA gives specific recommendations and suggestion that corporations can evaluate and implement (such as consent, data transfer, contractual obligations, etc.). The DPA provides the companies (specifically data controllers and processors) with guidelines on the new privacy regulation in order to let them implement the new requirements on time. The DPA will issue in the next few months further guidelines on the application of the GDPR.

General authorisation by the DPA

The DPA renewed on December 2016 the general authorisation for the processing of sensitive, genetic, judicial data and personal data processing for scientific research purposes. The authorisations are effective as of 24 May 2018. The DPA could release alternative authorisations or guidelines with regard to those processing after the abovementioned date.

Transfer of personal data by way of Privacy Shield

During this semester the DPA has also authorised the transfer of personal data to US companies that adhere to the Privacy Shield.

Cyber-bullying law

On May 2017, Italy adopted a law to combat cyber harassment, allowing young people who are bullied online to have comments removed in order to prevent teenage suicides (law no. 71, 29 May 2017 – effective from 18 June 2017).

Under the new law, teenagers over 14 years old and parents of younger children can now directly require an internet hosting provider or social network hosting abusive comments to delete them. If the offensive content is still visible and available after 48 hours, victims can appeal to the Data Protection Authority which will act within 48 hours from the receipt of the request.

Each school will have a reference teacher for combatting cyber harassment, with guidelines updated every two years by the education Ministry. School management has to promptly inform the families of the children involved in cyber bullying cases. In the absence of accusation by the victim or a criminal complaint (report the offence to the police) the bully will be subject to a warning by the Judicial Authority. The effect of the warning will cease at the age of 18.

Big Data

On 30 May 2017, the Italian Data Protection Authority**,** Antitrust Authority and the Communication Regulatory Authority (AGCOM) initiated a joint inquiry in order to evaluate criticalities on the use of big data and to define a set of common rules to protect personal data, digital economy and consumers.

Poland

Maria Guzewska, Associate, Marian Giersz, Associate & Piotr Dynowski, Partner, Bird & Bird, Warsaw office

The Polish regulator verifies marketing consent clauses used by banks

The Polish Inspector General for Personal Data Protection ("**GIODO**") has recently published a report showing consolidated findings from a series of internal data protection audits that were carried out at 20 banks.

In 2016 GIODO made formal requests to Data Protection Officers appointed at 20 banks in Poland to perform audits in order to verify lawfulness of personal data processing in the context of direct marketing to existing and potential clients. GIODO exercised their powers based on art. 19b of the Polish Data Protection Act – instead of carrying out an inspection by GIODO, the formally appointed and registered DPOs carried out the checks on GIODO's behalf and reported their findings directly to GIODO.

The audits focused on verification of legal grounds for the personal data processing, in particular the form in which consent for marketing is granted by existing and potential clients. GIODO identified the issue of combining **multiple consent clauses for marketing purposes as the most common mistake**. In particular, GIODO found that banks very often combine two or more of the following:

(a) consent for personal data processing for the purpose of own products marketing ;
(b) consent for personal data processing for the purpose of marketing of third party products;
(c) consent for e-communication;
(d) consent required under Telecommunications Law (in particular consent for telephone/SMS communication).

GIODO emphasized that consent for the personal data processing for marketing purposes should be separate from any other statements and clauses – in particular from consent for e-communication and the consent required under Telecommunications Law.

GIODO emphasized that if the consent clauses are combined, then the data subject cannot freely decide on how his/her data are used.

The approach is not a new one – the importance of providing separate consent clauses for different purposes has on many occasions been emphasized by GIODO and confirmed in judgments of administrative courts.

GIODO initiated administrative proceedings against banks which resulted in issuing administrative decisions ordering banks to rectify the improprieties.

Singapore

Cheng Hau Yeo, Associate, Daniel Song, Associate & Alexander Shepherd, Partner, Bird & Bird, Singapore office

Update to Personal Data Protection Commission guidance

On 28 March 2017, the Personal Data Protection Commission ("**PDPC**") published a revised version of its Anonymisation Advisory Guidelines ("**Guidelines**") issued under the Personal Data Protection Act ("**PDPA**"). Under the Guidelines, the PDPC has clarified that the standard to be applied in considering whether personal data has been anonymised is whether there is a serious possibility (or in the case of highly sensitive personal data, a less than serious possibility) that an individual could be re-identified. The Guidelines also set out certain factors to be considered in assessing the risks of re-identification. Additionally, organisations are also advised to implement controls to limit access to other information that could enable re-identification. Depending on the level of risk and complexity of issues, such controls could range from simple common sense methods to more complex measures. The Guidelines also clarify that any unintentional re-identification by an organisation is generally not considered as collection of personal data. However, any subsequent use or disclosure of such re-identified personal data will be subject to the PDPA.

There have also been revisions to other guidelines issued by the PDPC, which include the: (i) update of the advisory guidelines for the healthcare sector for greater clarity on service reminders; (ii) update of the Guide to Securing Personal Data in Electronic Medium and Guide to Disposal of Personal Data on Physical Medium to provide new examples of good practices in the handling of personal data for organisations; and (iii) update of the Guide on Building Websites for SMEs to include guidance on the use of ready-made software, which recommends organisations to understand the software features and how it should be configured to handle personal data.

UAE

New DP obligations in new digital payment services regulation

The Regulatory Framework for Stored Values and Electronic Payment Systems ("**EPS Regulations**") was published on 1 January 2017. The EPS Regulations introduce data protection and data storage regulations to those providing digital payment services in the UAE. Those offering digital payment services in the UAE must store user and transaction data ("**Data**") in the UAE for 5 years from the date the user relationship ends or the transaction date.

This Data must be protected and can only be made available to the user, Central Bank, other regulatory authority upon authorisation by the Central Bank, or by UAE court order. All such Data must also be physically stored in the UAE and therefore transfer of such Data outside of the UAE is restricted.

Digital payment services providers are not permitted to process the Data unless it is for the purposes of Anti-Money Laundering or Combatting the Financing of Terrorism checks. From the wording of the EPS Regulations, it appears that the transfer of the Data outside of the free zone where the servers are located is permitted; it is the transfer outside of the UAE that is prohibited.

Digital payment service providers have until 1 January 2018 to ensure they are compliant with these regulations.

Transfers to the US in light of the Schrems ruling (DIFC specific)

Please note that the Dubai International Financial Centre ("**DIFC**") is a free zone and has its own separate laws from the rest of Dubai ("**Onshore Dubai**").

Pursuant to the ECJ Schrems ruling on 6 October 2015, the commissioner of Data Protection for the DIFC released a statement informing companies incorporated in the DIFC that:

(a) they must protect individuals' personal data when it is transferred to the US and to consider the potential risks by implementing appropriate legal and technical solutions in a timely manner; and

(b) it is recommended that personal data transfers to the US should rely on alternative data transfer mechanisms provided by Article 12 of the DIFC DP law (these include the grounds for transfer under various EU laws such as consent, necessity in order to fulfil contract etc.) until there is further clarity emanating from the EU-US negotiations on devising an improved Safe Harbour framework.

There have been no further statements on this topic by the DIFC data protection commissioner but from the reading of his statement in October 2015, we can assume that the entities in the DIFC can rely on the new Privacy Shield scheme for transfer of personal data to the US. This remains to be seen.

United Kingdom

ICO feedback request on profiling and automated decision making

In April 2017 the ICO published a paper requesting feedback on the new profiling and automated decision making provisions in the General Data Protection Regulation (GDPR).

The paper is not formal guidance or a code of practice, but rather sets out the ICO's initial thoughts on the key areas of profiling it feels need further consideration, and requests feedback from interested parties. Some of the issues covered may be developed further when the Article 29 Working Party publishes its formal guidelines on profiling later this year. In the meantime, we highlight below some of the key points from the ICO's paper:

- organisations need to keep profiling activities under regular review to ensure that all the information obtained is relevant for the intended purpose, and that irrelevant data is not retained for longer than necessary;

- as profiles tend to comprise derived or inferred data, rather than data collected from the individuals themselves, there is a risk that organisations will infer sensitive personal data from non-sensitive personal data (e.g. inferring the state of an individual's health from the contents of their shopping trolley). This presents a challenge as sensitive personal data can generally only be processed with the explicit consent of the individual concerned;

- the GDPR requires that organisations provide individuals with meaningful information about the logic involved in an automated decision making process. The ICO interprets this requirement as meaning that information should be provided about how profiling might affect a data subject generally, rather than requiring information to be given about a specific decision. It also makes clear that this does not involve providing a detailed technical description, but rather involves clarifying the categories of personal data used, the source of the data, and why the data is considered relevant;

- the GDPR gives individuals the right to object to profiling. Where they do so, organisations must demonstrate compelling legitimate grounds if they are to override the objection. The ICO states that individuals must be clearly told about their right to object to profiling and this explanation should not be concealed with a set of general terms and conditions. Organisations must therefore be ready to justify their processing activities in readiness for an objection;

- in certain circumstances, individuals can object to decisions being made about them with are based solely on automated processing. The ICO interprets this to cover those automated decision making processes where a human exercises no real influence on the outcome of the decision;

- the GDPR is concerned with profiling which has a "legal" or "significant" effect on an individual. The ICO interprets "significant" as meaning a consequence that is more than trivial and potentially has an unfavourable outcome. This appears to be a reasonably low threshold;

- organisations must carefully consider how to ensure profiling is fair and non-discriminatory and does not have an unjustified impact on individuals. The ICO highlights the fact that profiling is often a continuous, evolving process, with new correlations in data sets discovered all the time. This means businesses must introduce appropriate measures to correct errors and minimise the risk of bias or discrimination. Such measures might include algorithmic 10 Date Description auditing, seals, codes of conduct and ethical review boards to underpin profiling safeguards; and

- before undertaking many profiling activities, organisations will need to undertake a Data Protection Impact Assessment (DPIA). The ICO gives credit scoring, insurance premium setting, location tracking, loyalty programs and behavioural advertising as examples of activities likely to require a DPIA. The ICO also says that DPIAs may be needed in the case of a decision making process which is only partially automated, if it results in a legal or significant effect on the individual.

The paper asks a number of specific questions for feedback. If you wish to feedback, the deadline for responding is 28 April 2017. Alternatively, you can use the ICO's paper to issue spot ahead of the release of more formal guidelines later this year.

ICO guidance on Big data, artificial intelligence, machine learning and data protection

In March 2017 the ICO published a discussion paper on big data, artificial intelligence, machine learning (collectively referred to as "big data analytics") and data protection. The paper is not formal guidance or a code of practice, but rather gives views on the implications of big data analytics for data protection law, and suggests some potential routes to compliance.

We expect that the Article 29 Working Party will publish their GDPR guidance on profiling and consent later in 2017, and the principles in this paper may well be developed in that guidance.

According to the ICO, big data analytics represents a step change from traditional personal data processing activities. In particular, the ICO identifies the use of algorithms, the opacity of the decision making process, the tendency to collect 'all the data', the repurposing of data sets and the use of new types of data as distinctive aspects of big data analytics that pose new compliance challenges.

The paper identifies a number of specific challenges, including:

- maintaining the overall fairness of personal data processing given the intrusive effects of certain types of big data analytics, such as profiling;
- aligning big data processing with the reasonable expectations of the individuals concerned;
- explaining complex methodologies and algorithms in a way that ensures organisations are transparent about what they are doing, and can obtain consent from individuals that is properly informed; and
- the issue of hidden biases in datasets leading to inaccurate predictions about individuals, or to discriminatory and unjustified decisions being made.

Perhaps of most interest is the ICO's view on the new right in the GDPR which allows individuals to obtain an explanation of decisions based on automated processing. For example, such automated decisions could be made in the context of credit applications, recruitment activities or insurance. The challenge here is that machine learning algorithms may learn and make decisions in a way that is "without regard for human comprehension", rendering it extremely difficult to provide a meaningful response to an individual who is exercising this new right. The ICO says that organisations must exercise caution before using technologies to make decisions where the methodology cannot be expressed in an understandable way. The suggestion here seems to be that if a decision has a significant effect on an individual, and the decision making methodology cannot be explained, then the technology should not be used.

Avoiding unintentional discrimination is crucial to complying with the law. By way of illustration, the paper refers to a study of a machine learning tool used in some US states to predict the future criminality of defendants. The study of the tool revealed that black defendants were falsely classified as future criminals on nearly twice as many occasions as white defendants, despite there being no intention to discriminate.

However, it is not enough to detect discrimination in hindsight and take steps to improve the technology. Businesses must have robust measures in place to detect potential discrimination prior to the use of big data analytics, and analysts must build anti-discriminatory measures into the technology at the planning stage.

The paper states that organisations can overcome these challenges by developing flexible and innovative compliance tools, including:

- using anonymised data only, coupled with robust risk assessments to mitigate the risk of individuals being re-identified from the data;
- putting in place new forms of privacy notices (e.g. videos, standardised icons, and 'just in time' notices) designed to help make complex information easier to understand;
- putting in place internal and external "algorithmic auditing" processes, to enable third parties to check and monitor the behaviour of an algorithm and the potential for bias and discrimination within the decision making process;
- using ethics boards within organisations which ensure the application of big data standards and principles and build trust with individuals; and
- undertaking formal privacy impact assessments to identify and mitigate privacy risks and assess the proportionality of big data processing.

The main conclusion of the paper is that whilst it is more difficult to apply data protection principles to big data analytics, tools exist and will continue to be developed to support compliance. The ICO's view is that the benefits of big data analytics will only truly be felt when data privacy is embedded in the methods by which such technologies are used.

Therefore whilst the use of big data analytics represents a significant change in the nature of processing activity, there is no doubt that data protection authorities intend to enforce compliance with the law within the framework of existing principles.

ICO Guidance for Consent in the GDPR

On 2nd March 2017, the ICO published draft guidance on consent under the General Data Protection Regulation. The consultation period for the guidance closed on 31 March 2017.

ICO's proposal to issue guidance on consent is a good idea: it is unrealistic to expect many organisations to read the text of GDPR, so this will make more people aware of the requirements in GDPR. It will also help to show the ICO's thinking on provisions in GDPR which are unclear.

There are good attempts to summarise and explain GDPR. However, the guidance is repetitive (so unnecessarily long). It also lapses into jargon in places. For those familiar with data protection this doesn't matter. However it risks making the guidance confusing or misleading for those who aren't. The frequent references to 'opt-in consent' are a good example of this.

Some of the examples used to illustrate points are also badly chosen – leading to over-complicated analysis, or missing industry specific nuances relevant to that example.

The guidance is an interesting first draft, but needs work. For the details, read on.

To opt-in, or not to opt-in?

Consent has to include an affirmative action by the individual. This is not new: the current Directive already states that the individual must 'signify agreement'.

It is tempting to abbreviate the requirement for consent to be active as 'opt-in consent'. However, this can lead to confusion: the Regulation does not state that consent has to involve use of a tick box; consent can be affirmed in many ways.

In the at-a-glance summary, the guidance state states that 'consent requires a positive opt-in'. This is unfortunate and risks confusing. (Elsewhere the guidance does make clear that this is just one way of obtaining consent, but the term risks misleading).

Renewing consent

If an organisation has already obtained consent, will it need to 'refresh' this in order to meet its obligations under GDPR? ICO draws attention to recital 171, which provides that there is no specific obligation to obtain new consent. However, if existing expressions of consent do not meet the standards set out in GDPR then they will not be valid: the organisation will need to ask for consent again, or find another justification to process personal data.

Real choice

The guidance summarises GDPR requirements that individuals must have a real choice for consent to be valid. They must also be able to revoke consent without detriment.

Helpfully, the guidance does accept that data controllers can offer a benefit, or an incentive, to people who give consent – and, if someone withdraws consent, the loss of this benefit will not render the consent invalid (on the basis that the individual suffers a detriment). The guidance gives the example of a scheme giving money-off vouchers to customers who agree to receive marketing materials. If you withdraw consent you lose the vouchers, but this would not make the request for consent invalid.

Separate from terms and conditions

GDPR requires that consent must be 'distinguishable'. ICO explains this means that consent should be separate from terms and conditions. ICO also highlights the GDPR requirement that an individual should not be required to give consent, as a condition of signing up to a service, unless the processing for which consent is sought is necessary for that service. This does not automatically make the consent invalid: however, there will be a presumption that it is not freely given.

Granular

Recital 43 of GDPR provides that '*consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case...*'. By way of an example, an insurance company may ask for consent to process health information which is necessary for it to evaluate risk in a life insurance contract. It may also ask for consent to send email marketing from group companies. These are different processing operations and it would be appropriate for the company to ask for consent separately – so as to allow me to request a quote, whilst saying no to marketing. ICO calls this concept 'granular consent'.

The example above is clear. However, it is easy to come up with difficult examples – for example, an organisation may carry out marketing by post, email and phone; it may also market its own products and those of third parties; and it may share lists with third parties: are these different processing operations, or are they all marketing? And if they are separate, how many options would the organisation have to present?

ICO draws attention to this provision, but does not give examples of occasions when it would be appropriate to offer separate choices and when it would not. ICO merely notes that there is no need to offer separate choice if this would be 'unduly disruptive or confusing'. In so far as it goes this is useful, as it recognises that an excess of choice may not be helpful.

Revocable

It must be as easy to withdraw consent as it is to give it – simple mechanisms are needed.

Proof

The guidance repeats GDPR requirements that an organisation must be able to demonstrate that it has obtained consent. There are some helpful lists of what this may require – such as keeping details of the versions of forms used.

Public bodies and employers

ICO notes that they are unlikely to be able to rely on consent, because of the imbalance in the relationship between the organisation and the individual which makes it unlikely that consent is freely given. There can be occasions when consent is freely given (for example, support services offered by an employer). It would be useful if the guidance recognised that this could be the case in some occasions.

Children

GDPR provides that if an online service is provided to a child and personal data is processed based on consent, then reasonable attempts must be made to obtain verifiable parental consent. There is a section in the guidance covering these rules. It also notes that consent given by a parent will expire once the child is old enough to give consent for him or herself.

Naming all third parties

The guidance states that the consent must name all third parties who will be relying on consent. This is both unclear and problematic. It is not clear whether the guidance means that organisations who ask for consent to share personal data with other organisations cannot share data unless they have listed all third parties. Alternatively, the guidance could be considering the situation of organisations who do not have a direct relationship with the individual, but who want to rely on consent as a lawful basis for processing, and who need the data controller with the initial relationship with the individual to obtain consent which covers their processing of personal data.

Whichever scenario is meant, the guidance is problematic: listing all third parties will be difficult for many businesses which rely on being able to share data, or which rely on others to obtain consent which covers their personal data processing. Use of data by direct marketers and by medical researchers is two obvious areas which will be adversely affected by this.

The guidance suggests that naming third parties is required for consent to be 'specific'. However, the Data Protection Directive also required consent to be specific and ICO did not previously suggest that this meant that all third parties had to be named.

Recital 42 does state that for consent to be informed, the individual must be aware of the identity of the person to whom consent is given (amongst other matters). However, this does not necessarily mean listing all third parties: it may be possible to meet this requirement by a clear description of a class of persons and a mechanism to provide more detail on request.

Wrong

Some bits of the guidance are just wrong. For example, it says that the requirement that consent must be 'unambiguous' is new (it isn't: it's in Article 6 of the Directive). The guidance also says that 'you are likely to need consent under ePrivacy laws for most marketing calls or messages...' in fact, most marketing calls do not need consent.

Data protection is not the only consideration

The guidance includes examples to illustrate the points made. Some of these are badly chosen – as the approach taken to consent is driven by non-data protection related considerations. ICO gives the example of:

- A company providing credit cards which asks customers to give consent for their personal data to be sent to a credit reference agency, to provide information on credit risk. ICO states that if the customer withdraws consent, the credit card company will still send the data, on the basis of its legitimate interests. On this basis, ICO advises not trying to ask for consent as it is misleading. Organisations providing credit cards are subject to duties of confidentiality (in addition to data protection obligations) which restrict their ability to share personal data. Although there are exceptions to this duty, which allow data to be shared where it is in the best interests of the bank, the limits of the exception are unclear, so it is typical to ask for consent in order to meet concerns about confidentiality.

- A healthcare provider, processing health data on the basis of implied consent. ICO chooses this example to illustrate the point that consent which meets the standard for another area of law (here: confidentiality) will not necessarily meet the requirements for consent under GDPR. ICO's conclusion is that '*..assumed implied consent would not ... qualify as explicit consent for special category data*'. The point is correct. However, the explanation is not clear and depends on use of industry jargon. The argument will be clear (and familiar) to those who deal regularly with health-care related data protection and confidentiality considerations (who will already know the point). It risks confusing the non-expert reader for whom the guidance is presumably written.

What about Brexit?

GDPR will, of course, come into force before the UK leaves the EU. However, after Brexit, there would be scope for the UK to change course if it wanted to – although there would be strong arguments for maintaining consistency in many areas (to allow consistency for business and to support UK claims to be an adequate country to which EU data can be transferred).

The ICO appears to want to stay with the EU-pack – noting that it intends the guidance to evolve as future guidance is issued by European data protection authorities.

Style-buster:

Warning for those sensitive to the use of the English language: the draft guidance introduces some new (and not altogether good) phrases. Our top picks are:

- 'Doing consent' - let's hope this isn't also used from the perspective of the individual – imagine having consent done to you;
- 'Consent mechanisms' - think Heath-Robinson contraptions;
- 'Consent requests' – which sound overly social-media specific;
- 'granular consent' (which sounds like a sweetener, but is good) and 'blanket consent' (which sounds cosy, but is bad);
- 'Consent as an organic, on-going and actively managed choice'- which sounds like an advert for health-food;
- '..keep your consents under review and refresh them' – which sounds like gardening advice; and
- 'Transparent privacy notices' – as opposed to ones which are translucent, or, even worse, opaque.

UK Government publishes review of UK cyber security landscape

In December 2016, the Government published its conclusions of a review (*'Cyber Security Regulation and Incentives Review'*) of the adequacy of the current UK cyber security landscape in the context of the wider economy (i.e. not essential service sector-specific). The headline to take from this report is that it seems very likely that the UK will implement the Network and Information Security (NIS) Directive notwithstanding the result of the 23 June 2016 referendum, stating that "[whilst the] Government is separately considering whether additional regulation might be necessary for critical sectors, including in the context of the NIS Directive due to be implemented in 2018 as well as wider national infrastructure considerations...The detailed scope and security requirements for NIS implementation will be set out by Government in 2017, informed by the work of the NCSC and lead Government departments with relevant sectors alongside broader Government consideration of critical infrastructure". This being said, the focus of this report was essentially whether the Government needed to introduce additional regulation above that which will be imposed on businesses (generally) under the General Data Protection Regulation ("**GDPR**") when it comes into force on 25 May 2018.

The Government's conclusion is clear: "For now, Government will not seek to pursue further general cyber security regulation for the wider economy over and above the GDPR. It should ultimately be for organisations to manage their own risk in respect of their own sensitive data (e.g. intellectual property) and online presence". The Government states that there is a "strong justification for regulation to secure personal data as there is a clear public interest in protecting

citizens from crime and other harm, where it may not otherwise be in organisations' commercial interests to do so". However, it reserves its role to improving/ enhancing this protection by means of its implementation of the GDPR. The reasons for not adding to the GDPR's red-tape are as follows:

1. It is satisfied that both the data breach notification obligations which will be imposed on both controllers and processors, and the "aggravating and mitigating factors affecting the size of fines imposed for cyber security related breaches", under the GDPR are sufficient means of effectively incentivising "organisations to adopt good cyber security practices".

2. Various measures will be implemented in due course which are designed to connect the field of data protection with the field of cyber security, for example, the collaboration of the ICO and the National Cyber Security Centre on relevant projects.

3. Government intervention must be proportionate: "It does not want to overburden businesses and organisations with unnecessary regulatory requirements".

This does not mean that businesses should become complacent: in addition to beginning to devise and implement data breach detection and notification procedures and policies, they must devise and implement "formal incident response plans to deal with hackers and the consequences" i.e. procedures dealing with the full 'life cycle' of a breach and its consequences